Hewlett Packard Enterprise

HPE 5130EI-CMW710-R3507P10 Release Notes

Contents

List of tables

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE 5130EI-CMW710-R3507P10. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE 5130EI-CMW710-R3507P10 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 3507P10

Note: You can see the version number with the command **display version** in any view. Please see **Note①**.

Version history

IMPORTANT:

The software feature changes listed in the version history table for each version are not complete. To obtain complete information about all software feature changes in each version, see the *Software Feature Changes* document for this release notes.

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
R3507P10	R3507P09	2023-03-09	Release	This version fixed bugs
R3507P09	R3507P02	2023-02-03	Release	This version fixed bugs.
R3507P02	R3507	2021-09-29	Release	This version fixed bugs.
R3507	R3506P11	2021-06-08	Release	This version fixed bugs and introduced feature changes. New features include: • EAD assistant
R3506P11	R3506P10	2021-01-29	Release	This version fixed bugs.
R3506P10	R3506P08	2020-11-12	Release	This version fixed bugs and introduced feature changes. New features include: • Configuring the 802.1p priority for control packets sent by a device • Packet spoofing logging and filtering entry logging for SAVI • Configuring password control over weak passwords • Enabling password change prompt logging

Version number	Last version	Release Date	Release type	Remarks
				Fixed bugs.
R3506P08	R3506P06	2020-07-27	Release	This version fixed bugs.
R3506P06	R3506P02	2020-06-19	Release	This version fixed bugs and introduced feature changes. New features include: • Enabling recording untrusted DHCP servers on a DHCP snooping device There are also modified features. Fixed bugs.
R3506P02	R3506	2019-12-23	Release	This version fixed bugs.
R3506	R3208P16	2019-07-12	Release	This version fixed bugs and introduced feature changes. New features include: • For more information about the new features, see *HPE 5130EI-CMW710-R3506 Release Notes (Software Feature Changes)* There are also modified features. Fixed bugs.
R3208P16	R3208P15	2019-03-15	Release	This version fixed bugs and introduced feature changes. New features include: • Setting the block timer for MAC addresses in the blocked MAC address list • Logging off 802.1X users • Logging off MAC authentication users Fixed bugs.
R3208P15	R3208P12	2018-12-26	Release version	This version fixed bugs and introduced feature changes. New features include: • Configuring zero-to-two VLAN mapping • Specifying DNS server information in RA messages • Specifying DNS suffix information in RA messages • Suppressing advertising DNS information in RA messages • HTTP redirect • ERPS There are also modified features. Fixed bugs.
R3208P12	R3208P10	2018-09-26	Release version	This version fixed bugs and introduced feature changes. New features include:

Version number	Last version	Release Date	Release type	Remarks
				• PD detection mode There are also modified features. Fixed bugs.
R3208P10	R3208P08	2018-08-29	Release version	This version fixed bugs and introduced feature changes. New features include: • Automatic obtaining of the login username for temporary user role authorization • 802.1X EAP-TLS fragmentation for packets sent to the server • Enabling interface consistency check for ARP and MAC address entries • 802.1X offline detection • Enabling SAVI and setting the entry deletion delay by using commands There are also modified features. • Fixed bugs.
R3208P08	R3208P03	2018-05-22	Release version	This version fixed bugs and introduced feature changes. New features include: • Shutting down an interface by OpenFlow There are also modified features. • Fixed bugs.
R3208P03	R3208	2017-12-20	Release version	This version fixed bugs and introduced feature changes. New features include: • VRRP There are also modified features.
R3208	R3207	2017-08-15	Release version	This version fixed bugs and introduced feature changes. New features include: • MAC address information display for 802.1X users in 802.1X VLANs of a specific type • Authorization CAR action in an ISP domain • 802.1X client There are also modified features.
R3207	R3115P08	2017-04-27	Release version	This version fixed bugs and introduced feature changes. New features include: • Fundamentals features • IRF features • Layer 2-LAN switching features There are also modified features. Fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R3115P08	R3115P07	2017-03-20	Release version	This version fixed bugs and introduced feature changes. New features include: • ISP domain for users assigned to nonexistent domains Fixed bugs.
R3115P07	R3115P06	2017-02-16	Release version	Modified feature: • The login success message for 802.1X users • The login failure message for 802.1X users Fixed bugs.
R3115P06	R3115P05	2016-12-22	Release version	New feature: • 802.1X MAC address binding Modified feature: • Password configuration for MAC authentication MAC-based user accounts • Setting the fixed-area ratio for a queue • Setting the maximum shared-area ratio for a queue • Setting the total shared-area ratio • Burst feature Fixed bugs.
R3115P05	R3115P03	2016-10-24	Release version	Modified feature • Operating information collection • Maximum length of jumbo frames allowed by an Ethernet interface • Controlling SSH client access to the SSH server • Debugging switches Fixed bugs.
R3115P03	R3115P01	2016-09-27	Release version	Modified feature • Configuring a test profile for RADIUS server status detection • NTP support for ACL Fixed bugs.
R3115P01	R3115	2016-08-16	Release version	New feature • Configuring traffic policing for all incoming traffic by using the non-MQC approach • Bandwidth guaranteeing group • Ignoring the ingress ports of ARP packets during user validity check Modified feature Fixed bugs.
R3115	R3113P05	2016-07-15	Release version	New features • Including user IP addresses in

Version number	Last version	Release Date	Release type	Remarks
				realtime accounting packets for MAC authentication users with dynamic IP addresses • Configuring periodic MAC reauthentication Modified feature: • Kernel thread deadloop detection Fixed bugs.
R3113P05	R3113P03	2016-06-15	Release version	New features • PD detection mode Fixed bugs.
R3113P03	R3113P02	2016-05-27	Release version	Fixed bugs.
R3113P02	R3112	2016-05-06	Release version	New features • Automatic negotiation for speed downgrading • RADIUS stop-accounting packet buffering • HWTACACS stop-accounting packet buffering • Support of 802.1X for redirect URL assignment • Support of MAC authentication for redirect URL assignment • Support of port security for redirect URL assignment in specific modes • SAVI Modified feature • CDP compatibility for LLDP Fixed bugs.
R3112	R3111P07	2016-03-18	Release version	Modified feature • Displaying the number of online 802.1X users • Displaying the number of online MAC authentication users • Displaying the number of online Web authentication users Fixed bugs.
R3111P07	R3111P03	2016-02-03	Release version	New feature • Enabling bridging on an Ethernet interface • Sending EAP-Success packets to 802.1X users in critical VLAN • Triple authentication • Enabling SNMP notifications for port security • Enabling SNMP notifications for RRPP Modified feature • Configuring the HTTPS listening port number for the local portal

Version number	Last version	Release Date	Release type	Remarks
				Web server • Specifying ECDSA algorithms with different public key lengths • Fixed bugs.
R3111P03	R3111P02	2015-12-31	Release version	New feature • Web authentication • Allowing link aggregation member ports to be in the deployed flow tables • Transceiver module alarm suppression Modified feature • 802.1X guest VLAN assignment delay Fixed bugs.
R3111P02	R3111P01	2015-12-28	Release version	Fixed bugs.
R3111P01	R3110	2015-12-18	Release version	Fixed bugs.
R3110	R3109P16	2015-11-30	Release version	New features: • Enabling SNMP notifications for new-root election and topology change events • IP address pool authorization by AAA • Port-specific 802.1X periodic reauthentication timer • Manual reauthentication for all online 802.1X users on a port • IPsec support for Suite B • SSH support for Suite B • Public key management support for Suite B • PKI support for Suite B • SSL support for Suite B Modified feature: • FIPS self-tests • Configuring the CDP-compatible operating mode for LLDP Fixed bugs.
R3109P16	R3109P14	2015-11-17	Release version	New features: • Packet Capture Fixed bugs.
R3109P14	R3109P09	2015-10-31	Release version	New features: • Including client IP addresses in realtime accounting packets for 802.1X clients with dynamic IP addresses • Enabling MAC authentication multi-VLAN mode on a port • RADIUS DAE server

Version number	Last version	Release Date	Release type	Remarks
				• RADIUS server status detection • RADIUS server load sharing • 802.1X guest VLAN assignment delay • Sending 802.1X protocol packets without VLAN tags • 802.1X critical voice VLAN • MAC authentication critical voice VLAN • Parallel processing of MAC authentication and 802.1X authentication • RA guard logging feature • Displaying RA guard statistics • Clearing RA guard statistics • Configuring log suppression for a module Modified features: • 802.1X command output • MAC authentication command output • Displaying interface information • Configuring the types of advertisable LLDP TLVs on a port • Specifying RADIUS servers • Configuring SSH access control Removed features: • Enabling PoE for a PSE • Fixed bugs. • HPE rebranding
R3109P09	R3109P07	2015-9-14	Release version	New features: • L2PT Fixed bugs.
R3109P07	R3109P05	2015-7-31	Release version	New features: • MAC authentication offline detection Fixed bugs.
R3109P05	R3109P04	2015-6-16	Release version	Fixed bugs.
R3109P04	R3109P03	2015-5-28	Release version	Fixed bugs.
R3109P03	R3109P01	2015-5-15	Release version	New features: • RA Guard Modified feature: Configuring the TCP maximum segment size (MSS) Fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R3109P01	R3108P03	2015-4-2	Release version	New features: • RADIUS voice VLAN attribute for 802.1X and MAC authentication • 802.1X online user handshake reply Modified feature: • Specifying startup images Fixed bugs.
R3108P03	R3108P01	2015-2-13	Release version	New features: • Disabling SSL 3.0 • Login delay • ND Snooping Fixed bugs.
R3108P01	R3106	2014-12-12	Release version	Fixed bugs.
R3106P01	R3106	2014-8-9	Release version	Add new hardware support
R3106	First release	2014-7-28	Release version	First release

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use Table 2 to verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	5130 EI Series
Hardware platform	HPE 5130-24G-4SFP+ EI Switch JG932A HPE 5130-24G-SFP-4SFP+ EI Switch JG933A HPE 5130-48G-4SFP+ EI Switch JG934A HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch JG936A HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch JG937A HPE 5130-24G-2SFP+-2XGT EI Switch JG938A HPE 5130-48G-2SFP+-2XGT EI Switch JG939A HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch JG940A HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch JG941A HPE 5130-24G-4SFP+ EI Brazil Switch JG975A HPE 5130-48G-4SFP+ EI Brazil Switch JG976A HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A

Item	Specifications
Minimum memory requirements	1 GB
Minimum Flash requirements	512 M
Boot ROM version	Version 147 or higher (Note: Use the **display version** command in any view to view the version information. Please see **Note②**)
Host software	5130EI-CMW710-R3507P10.ipe
iMC version	iMC BIMS 7.3(E0506H01) iMC EAD 7.3(E0611P10) iMC QoSM 7.3(E0505P01) iMC EIA 7.3(E0611P13) iMC PLAT 7.3(E0705P12) iMC NTA 7.3(E0707L06) iMC SHM 7.3(E0707L06)
iNode version	iNode PC 7.3(E0585)
Web version	None
Remarks	None

Display the system software and Boot ROM versions of 5130EI:

```
<Sysname>display version
HPE Comware Software, Version 7.1.070, Release 3507P10   ------ Note①
Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP
HPE 5130 24G 4SFP+ EI Switch uptime is 0 weeks, 0 days, 0 hours, 3 minutes
Last reboot reason : User reboot

Boot image: flash:/5130ei-cmw710-boot-r3507p10.bin
Boot image version: 7.1.070, Release 3507P10
  Compiled Sep 15 2021 11:00:00
System image: flash:/5130ei-cmw710-system-r3507p10.bin
System image version: 7.1.070, Release 3507P10
  Compiled Sep 15 2021 11:00:00


Slot 2:
Uptime is 0 weeks,0 days,0 hours,3 minutes
5130-24G-4SFP+ EI with 1 Processor
BOARD TYPE:          5130-24G-4SFP+ EI
DRAM:                1024M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.B
Bootrom Version:     147            ------ Note②
CPLD 1 Version:      001
Release Version:     HPE 5130 24G 4SFP+ EI JG932A-3507P10
Patch Version  :     None
Reboot Cause   :     UserReboot
[SubSlot 0] 24GE+4SFP Plus
```

Upgrade restrictions and guidelines

Before performing a software upgrade, it is important to refer to the *Software Feature Changes* document for any feature changes in the new version. Also check the most recent version of the related documents (see "Related documents") available on the HPE website for more information about feature configuration and commands.

Hardware feature updates

Hardware feature updates in R3507P10~R3115

None

Hardware feature updates in R3113P05

R3113P05 supports the following new hardware:

- Flashes that support 4-bit ECC check:
  - MICRON: MT29F4G08ABADAWP:D
  - SPANSION: S34ML01G200TFI003
- Flashes that support 8-bit ECC check:
  - MXIC: MX30LF4G28AB

Hardware feature updates in R3113P03~R3108P03

None

Hardware feature updates in R3108P01

Added support for HP 5130-24G-2SFP+-2XGT EI Switch JG938A,HP 5130-48G-2SFP+-2XGT EI Switch JG939A,HP 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch JG940A,HP 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch JG941A.

Hardware feature updates in R3106P01

Added support for HP 5130-24G-4SFP+ EI Brazil Switch JG975A,HP 5130-48G-4SFP+ EI Brazil Switch JG976A,HP 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A,HP 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A.

Hardware feature updates in R3106

- First release.

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5130EI-CMW710-R3507P02 Release Notes (Software Feature Changes).*

MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
5130EI-CMW710-R3507P10~5130EI-CMW710-R3506P11			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3506P10			
New	savi.mib	SAVI-MIB	Added the following objects to SaviObjectsSystemEntry: saviObjectsSystemNotifySpoofing used for setting or obtaining the status of packet spoofing logging. saviObjectsSystemNotifyFilter used for setting or obtaining the status of filtering entry logging. saviObjectsSystemNotifySpoofingInterval used for setting or obtaining the log output interval for packet spoofing logging. saviObjectsSystemNotifySpoofingNumber used for setting or obtaining the maximum number of log messages that can be output per interval. saviObjectsSystemBindingCount used for obtaining the number of binding entries. saviObjectsSystemFilteringCount used for obtaining the number of filtering entries. Added the following object to SaviObjectsCountEntry: saviObjectsCountFilterOctets used for obtaining the byte count for spoofed packets filtered by SAVI.
Modified	None	None	None
5130EI-CMW710-R3506P08~5130EI-CMW710-R3111P02			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3111P01			
New	hh3c-port-security.mib	HH3C-PORT-SECURITY-MIB	Added descriptions and support for the following Trap: hh3cSecureAddressLearned hh3cSecureViolation hh3cSecureLoginFailure hh3cSecureLogon hh3cSecureLogoff hh3cSecureRalmLoginFailure hh3cSecureRalmLogon hh3cSecureRalmLogoff

Item	MIB file	Module	Description
Modified	None	None	None
5130EI-CMW710-R3110			
New	hh3c-splat-inf-new.mib	HH3C-LswINF-MIB	Added descriptions and support for the following MIBs: hh3cifPktBufTable
	hh3c-lsw-dev-adm.mib	HH3C-LSW-DEV-ADM-MIB	Added descriptions and support for the following MIBs: hh3cLswSlotPktBufFree hh3cLswSlotPktBufInit hh3cLswSlotPktBufMin hh3cLswSlotPktBufMiss
Modified	None	None	None
5130EI-CMW710-R3109P16~5130EI-CMW710-R3109P03			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3109P01			
New	None	None	None
Modified	rfc1213-mib.docx	IP-MIB	ipForwarding (1.3.6.1.2.1.4.1) Only support read operation ipDefaultTTL (1.3.6.1.2.1.4.2) Only support read operation
5130EI-CMW710-R3108P03~5130EI-CMW710-R3106P01			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3106			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R3507P10

None

Operation changes in R3507P09

None

Operation changes in R3507P02

None

Operation changes in R3507

- When the number of MAC address entries learned on a port reaches the upper limit, the message generated for this issue has changes.
  - Before modification: The message is `The number of MAC address entries exceeded the maximum number.`
  - After modification: The message is `The number of MAC address entries reached the maximum number.`

Operation changes in R3506P11

- Excluded the *freeradius.bin* file from the IPE file.

Operation changes in R3506P10

None

Operation changes in R3506P08

None

Operation changes in R3506P06

The following commands were added to the default configuration file:

```
password-control enable
#
local-user admin
service-type terminal
authorization-attribute user-role network-admin
#
user-interface aux 1
authentication-mode scheme
#
undo password-control aging enable
undo password-control composition enable
undo password-control history enable
undo password-control length enable
password-control login idle-time 0
password-control login-attempt 3 exceed unlock
password-control update-interval 0
```

Operation changes in R3506P02

None

Operation changes in R3506

- Modified the 802.1p priority in the VLAN tags of ARP replies sent by the device from 0 to 6

Operation changes in R3208P16

None

Operation changes in R3208P15

- For the HPE 5130-24G-4SFP+ EI Switch JG932A and HPE 5130-24G-4SFP+ EI Brazil Switch JG975A, this version modified the start-to-work temperature for fans from 88°C to 98°C.
- For the HPE 5130-24G-2SFP+-2XGT EI Switch JG938A switches, this version modified the start-to-work temperature for fans from 83°C to 93°C.

Operation changes in R3208P12

- Adjusted the priority of the BFD MAD detection packets to optimize the BFD MAD feature.

Operation changes in R3208P10

None

Operation changes in R3208P08

Changed the ACL issuing operation

Before modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on client MAC addresses.

After modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on CLASS-IDs rather than client MAC addresses. The device uses the same CLASS-ID when issuing Layer 2 ACLs to authentication users with the same authorization ACL, which saves ACL resources.

Operation changes in R3208P03

- Modified the over-temperature protection feature.

When the switching chip junction temperature exceeds 107 °C, the switch displays a log and reboots.

Operation changes in R3208

None

Operation changes in R3207

Before the modification: A PoE switch enabled with LLDP does not perform any operations if it has not received any LLDP frames from a connected AP before the defined timer expires.

After the modification: A PoE switch enabled with LLDP power cycles the PoE port (PI) and reboots a connected AP forcibly if it has not received any LLDP frames from the AP before the defined timer expires.

Operation changes in R3115P08

- The **bpdu-drop any** command in Layer 2 Ethernet interface view added support for dropping PVST and PVST+ packets.

Operation changes in R3115P07

None

Operation changes in R3115P06

None

Operation changes in R3115P05

None

Operation changes in R3115P03

None

Operation changes in R3115P01

None

Operation changes in R3115

None

Operation changes in R3113P05

None

Operation changes in R3113P03

None

Operation changes in R3113P02

None

Operation changes in R3112

None

Operation changes in R3111P07

None

Operation changes in R3111P03

Added support on Port Security logging.

Operation changes in R3111P02

None

Operation changes in R3111P01

None

Operation changes in R3110

None

Operation changes in R3109P16

None

Operation changes in R3109P14

None

Operation changes in R3109P09

Changed the OpenFlow packet-in rate limit from 200 PPS to 1000 PPS.

Operation changes in R3109P07

The priorities of ACL resources were modified to save ACL resources.

Added support for issuing commands to an SSH server.

- Before modification, an SSH user cannot issue commands to a switch acting as an SSH server through SSH parameters.
- After modification, an SSH user can issue commands in batches to an SSH server through SSH parameters.

Operation changes in R3109P05

None

Operation changes in R3109P04

None

Operation changes in R3109P03

Added support for portal configuration in the Web interface

- Before modification, portal configuration is not supported in the Web interface.
- After modification, portal configuration is supported in the Web interface.

Operation changes in R3109P01

None

Operation changes in R3108P03

None

Operation changes in R3108P01

None

Operation changes in R3106P01

None

Operation changes in R3106

First release.

Restrictions and cautions

1. If the authorization VLAN does not exist, the access device first creates the VLAN and then assigns the user access interface as an untagged member to the VLAN. If the authorization VLAN already exists, the access device directly assigns the user access interface as an untagged member to the VLAN.

2. To deploy Web authentication on a trunk or hybrid port, make sure the port PVID, the authorization VLAN ID, and the user VLAN ID are the same.
3. The offline detect timer for MAC authentication and the aging timer for dynamic MAC address entries must be set to the same value.
4. When you downgrade a software package with the BootROM version 142 or a later version to a software package with the BootROM version earlier than 142, the BootROM version 122, 130, 132, or 134 is not downgraded together with the software package version.
5. When the HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch (JG940A) and HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch (JG941A) supply power to some telephones through PoE, you must use crossover cables.
6. When you configure 802.1X authentication and MAC authentication, follow these restrictions:
   a. When users with ACLs assigned exist on a single port, you must assign ACLs (for example, ACLs with the permit rule) to the users that do not need ACLs assigned. This operation ensures that these users do not mistakenly match ACLs of other users.
   b. You must adjust the ACL rule positions to ensure that the traffic of each online user can match rules in the ACL assigned to the user.
   c. When multiple users come online on a port and the same ACL is assigned to these users, to add rules to or delete rules from the ACL, you must first log off all users on the port and then add or delete ACL rules. Otherwise, some deleted ACL rules will remain.

Open problems and workarounds

None

List of resolved problems

Resolved problems in R3507P10

202303021705

- Symptom: The switch fails to forward PTP packets.
- Condition: This symptom occurs if PIM-DM and IGMP are configured on the switch.

Resolved problems in R3507P09

202212141432

- Symptom: A port might not come up.
- Condition: This symptom occurs if a 10-GE copper port operates at 1000 Mbps.

202209030500

- Symptom: The switch prints a log message that CRC errors packets were received.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable flow sampling and specify the number of packets out of which flow sampling samples a packet in Ethernet interface view.
  b. The packets received on the interface are sent to the CPUs of other IRF member devices through IRF physical links.

202208111206

- Symptom: PIM packets cannot be forwarded at Layer 2.

- Condition: This symptom occurs if IGMP snooping is enabled.

202208100206

- Symptom: The system might prompt insufficient ACL resources.
- Condition: This symptom occurs if a packet filter is applied to an interface and then rules in the ACL of the packet filter are modified.

202203290188

- Symptom: VLANs that do not belong to an AC interface are blocked.
- Condition: This symptom occurs if STP is enabled on the AC interface in an L2VPN network.

Resolved problems in R3507P02

202107110018

- Symptom: The aggregate interface configured as an MFF network port forwards received ARP requests out of its member interfaces.
- Condition: This symptom occurs if a Layer 2 aggregate interface is configured as an MFF network port after MFF is enabled.

202108250280

- Symptom: Batch backup fails to complete when BGP NSR backs up data from the active BGP process to the standby BGP process consecutively.
- Condition: This symptom might occur when BGP NSR backs up data from the active BGP process to the standby BGP process consecutively.

202107050836

- Symptom: Error logs about unsupported or unavailable transceiver modules are generated repeatedly, resulting in high CPU usage.
- Condition: This symptom occurs if the following conditions exist:
  - The device is installed with an incompatible transceiver module or not installed with any transceiver modules.
  - Network management software retrieves information about transceiver modules periodically.

202107211304

- Symptom: Failed to save the running configuration.
- Condition: This symptom might occur when you use the **`save`** command to save the running configuration.

202107191057

- Symptom: Some 802.1X users cannot come online on a port.
- Condition: This symptom might occur if the following conditions exist:
  - The port is enabled with both 802.1X authentication and MAC authentication.
  - A large number of users are repeatedly coming online and going offline.

202107211171

- Symptom: After you execute the **silent-interface all** command for the OSPF process, execute the **`undo silent-interface`** command for the OSPF interface, and restart the device, the configuration of the **undo silent-interface** command does not take effect, causing OSPF neighbor relationship establishment failures.

- Condition: This symptom might occur when you execute the **silent-interface all** command for the OSPF process, execute the **`undo silent-interface`** command for the OSPF interface, and then restart the device.

202107220559

- Symptom: BGP peer flapping with a packet loss duration of nine seconds occurs after an active/standby switchover, and error message **Send notification with error 5/0** is displayed.
- Condition: This symptom might occur when the following conditions exist:
  - An active/standby switchover occurs on the device.
  - The configuration on the BGP peer of the device changes during the switchover and the peer sends Refresh packets to the device.

202107110017

- Symptom: The aggregate interface sends a received ARP reply out of a member interface back to the upstream device, and the upstream device reports a MAC move event.
- Condition: This symptom occurs after the **`arp detection trust`** command is executed on an aggregate interface and the aggregate interface receives an ARP reply.

202108230830

- Symptom: The device falsely reports CRC error packet notifications for IRF ports.
- Condition: This symptom might occur if the device has been running for a period of time and a number of ports are forwarding traffic.

202109240201

- Symptom: All devices are elected as the master in the IPv6 VRRP group, and they cannot ping each another.
- Condition: This symptom occurs if you configure the **mld-snooping source-deny** command for a member port in a dynamic aggregation group.

202109240467

- Symptom: The system prompts that a QoS policy failed to be applied to an interface, and flow mirroring ERSPAN failed.
- Condition: This symptom occurs if you configure flow mirroring ERSPAN for an aggregation group member port and the aggregation group member port comes up and goes down multiple times.

202107160918

- Symptom: The lldp process might exit unexpectedly.
- Condition: This symptom might occur if aggregation groups exist on the device and the lldpLocManAddrEntry table in the MIB is regularly accessed.

202107191086

- Symptom: After some 802.1X users come online, no authorization VLAN or VSI is assigned to them.
- Condition: This symptom occurs if the following operations are performed:
  a. Both 802.1X authentication and MAC authentication are enabled on interface.
  b. ACLs are assigned to MAC authentication users.
  c. Users come online and then go offline.
  d. VLANs or VSIs are assigned to 802.1X users.

202103311306

- Symptom: Failed to delete a permanent static route.

- Condition: This symptom occurs if the following operations are performed:
  a. Configure a permanent static route and specify a preference lower than common static routes for the permanent static route.
  b. Change the output interface address of the permanent static route and change the permanent static route settings multiple times. The permanent static route is recursed to a common route or to Null 0.
  c. Delete the permanent static route.

Resolved problems in R3507

202105110200

- Symptom: CVE-2021-29219, an incorrect neighbor management address is displayed in the output from the **display lldp neighbor-information verbose** command.
- Condition: This symptom occurs if the following conditions exist:
  - The length of the value in the Management Address TLV is less than 8 bytes in the CDP packets received by the device.
  - The total length of the Management Address TLV is less than 12 bytes.

202104220726

- Symptom: User credential information leaks.
- Condition: This symptom might occur when the user logs in to the Web interface of the device.

202105060531

- Symptom: Host routes become invalid on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the host routes have different next hops.

202105110235

- Symptom: The number of secure MAC addresses on a port has reached the upper limit. However, port security does not work as expected when a user moves from another port to this port.
- Condition: This symptom occurs if the following operations are performed:
  a. Port security is enabled on both of the ports. On each of the ports, the MAC address of a user is configured as a secure MAC address. The secure MAC addresses configured on the two ports are different.
  b. The two ports learn MAC addresses from each other.
  c. The users that use the configured secure MAC addresses move between the two ports.

202103290727

- Symptom: The netmeisterd process runs abnormally on an IRF fabric.
- Condition: This symptom occurs if third-party network management software cannot correctly recognize the H3C IRF fabric and issues a command to reboot the master device of the IRF fabric.

202102230116

- Symptom: The DHCP address pool fails to assign IP addresses to clients from its second secondary subnet.
- Condition: This symptom might occur if no IP addresses are available for dynamic allocation on the primary subnet and first secondary subnet in the DHCP address pool.

202104200379

- Symptom: The device reboots unexpectedly after running for a period of time.

- Condition: This symptom occurs if the device receives IP packets destined to 239.255.255.250 and with the TTL as 1 or 2.

202102150008

- Symptom: The **netconf log source all verbose** command gets stuck on an IRF fabric with an extremely low probability.
- Condition: This symptom might occur after a master/subordinate switchover if the IRF fabric is configured with loop detection and AAA or NETCONF services exist on the IRF fabric.

202103241845

- Symptom: After you modify the device IP, the device can still access the network.
- Condition: This symptom occurs if the actual number of ARP snooping entries on the device is different from that collected by the counter.

202102160026/202102221454

- Symptom: Online MAC authentication users are logged out on an IRF fabric because their idle timeout timer expires. However, the users are continuously sending traffic to the device.
- Condition: This symptom occurs if a master/subordinate switchover has occurred on the IRF fabric.

202102100037

- Symptom: A number of MAC authentication users are logged out on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the online duration of these MAC authentication users is longer than the session timeout period assigned by the server after the master/subordinate switchover.

202104200312

- Symptom: MAC authentication users cannot come online on a port.
- Condition: This symptom might occur if the MAC authentication users come online and go offline repeatedly on the port when the following conditions exist:
  - The port is enabled with both 802.1X authentication and MAC authentication.
  - The port is configured with the 802.1X guest VLAN.

Resolved problems in R3506P11

202101190137

- Symptom: The device reboots automatically with a low probability when it runs the R3506P08 or R3506P10 software version. The reboot reason is reported as **UserReboot**.
- Condition: This symptom might occur when the device runs the R3506P08 or R3506P10 software version.

Resolved problems in R3506P10

202008260498

- Symptom: Port isolation does not take effect on an aggregate interface.
- Condition: This symptom might occur if port isolation is configured on an aggregate interface where multiple ACs exist.

202009220628

- Symptom: The device cannot identify phone offline events.
- Condition: This symptom might occur if the device is attached to phones that do not send CDP packets periodically, such as Polycom and AudioCodes phones.

202009280287

- Symptom: CVE-2020-10188
- Condition: utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.

202008240782

- Symptom: The Telnet process hangs.
- Condition: This symptom might occur if command accounting is enabled and the AAA server is unreachable.

202008240177

- Symptom: Users fail their first portal authentication attempts while passing the second one.
- Condition: This symptom might occur if both the **portal apply mac-trigger-server** and **portal apply web-server settings are** configured.

Resolved problems in R3506P08

202007271063

- Symptom: The device might fail to start properly with a very low probability.
- Condition: This symptom occurs if the device is repeatedly power-cycled.

Resolved problems in R3506P06

202005271313

- Symptom: 1-Gbps fiber ports do not come up.
- Condition: This symptom occurs because 1-Gbps fiber ports cannot be connected to SGMII devices.

202005291034

- Symptom: An aggregate interface does not load share TCP or UDP traffic among member links.
- Condition: This symptom might occur if TCP or UDP traffic is forwarded out of an aggregate interface.

202001170358

- Symptom: 802.1X users and MAC authentication users come online through the same port. The ACL issued to users that come online later does not take effect.
- Condition: This symptom occurs if the following operations have been performed:
  a. Configure both MAC authentication and 802.1X authentication on a port.
  b. Issue the same ACL to users.

202005111273

- Symptom: The combo ports on all IRF subordinate devices go down after a master/subordinate switchover.

- Condition: This symptom occurs if the master/subordinate switchover occurs after the original master device reboots or the entire IRF fabric reboots.

Resolved problems in R3506P02

202001080562

- Symptom: A MAC address cannot be learned into the corresponding VLAN.
- Condition: This symptom occurs if an IP subnet-based VLAN is configured and an interface in the VLAN receives packets with the same source MAC address.

201912170108

- Symptom: When the PoED process is restarted, the process does not respond.
- Condition: This symptom occurs if the following conditions exist:
  - Multiple PoE-capable devices form an IRF fabric.
  - The master and subordinate member devices all act as PSEs to supply power.
  - The PoED process is restarted every 20 seconds.

201911070588

- Symptom: The SSHD call stack might be printed.
- Condition: This symptom occurs if you log in to the device repeatedly through SSH.

201908270157

- Symptom: After a user passes 802.1X authentication and enters the username and password on a PC, ErrCode=0 appears on the switch and the user goes offline. About half a minute to one minute later, the user performs authentication again and comes online.
- Condition: This symptom occurs if the following operations are performed:
  - On an interface configured with port-based access control, configure the guest VLAN and the hybrid port is removed from the default VLAN (VLAN 1).
  - After a user passes 802.1X authentication, the user modifies the username and password and initiates authentication again.

Resolved problems in R3506

201906200052

- Symptom: The port security, LLDP, and interface management processes become deadlocked.
- Condition: This symptom occurs with a low probability if port security is configured on the device and an intrusion protection is triggered.

201906050407

- Symptom: When many-to-one VLAN mapping is configured on the device, a connected terminal cannot ping the extranet after it re-obtains an IP address.
- Condition: This symptom might occur if the terminal re-obtains the IP address after the port through which the terminal connects to the device is moved from an original VLAN to the translated VLAN.

201905080677

- Symptom: On an ADCampus network, the device obtains an incorrect automated VCF fabric deployment template.

- Condition: This symptom might occur if the device is an access node and tries to obtain an automated VCF fabric deployment template.

201904180672

- Symptom: IPv6-AH packets cannot match an ACL rule with the protocol specified as ipv6-ah.
- Condition: This symptom might occur if the protocol is specified as ipv6-ah for an ACL rule.

201904150324

- Symptom: When the device is configured to display log buffer information and buffered logs, it displays only the newest log rather than all logs in the log buffer.
- Condition: This symptom might occur if the display operation is repeatedly performed after the log buffer gets full.

201904100097

- Symptom: CFD loopback does not take effect on a service instance.
- Condition: This symptom might occur if the MAs in the service instance are configured without carrying the VLAN attribute.

201902020370

- Symptom: Only eight ports on the PoE-capable device can supply power.
- Condition: This symptom might occur if an exception exists on the power management configuration register.

201905140328

- Symptom: When port security is configured, traffic forwarding fails because of secure MAC address loss after the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.
- Conditions: This symptom might occur if the IRF fabric contains three or more member devices and the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.

Resolved problems in R3208P16

201902010586

- Symptom: CVE-2018-5407
- Condition: OpenSSL is prone to a local information-disclosure vulnerability. Local attackers can exploit this issue to obtain sensitive information. This may aid in further attacks.

201812070828

- Symptom: HPE Comware 7 stored and reflected XSS Vulnerability
- Condition: An xss reflected in the web portal of the appliance HP Comware switch 7.1.045. Attackers can exploit this issue to open a web browser and log in to the application using valid or not credentials.

201812280425

- Symptom: Multiple Telnet users remain and cannot be deleted, and the CPU usage keeps higher than 50% as a result.
- Condition: This symptom might occur if the Telnet window is closed when a Telnet user logs in to a comsh user and then logs in to a Telnet user.

201812280404

- Symptom: The sshd process deadlock occurs.
- Condition: This symptom might occur if SSH logout is performed when the CPU usage is high.

201812250322

- Symptom: The **arp restricted-forwarding enable** command might not take effect.
- Condition: This symptom occurs if the **arp restricted-forwarding enable** command is configured on the device and the device uses IPSG bindings for forwarding preferentially.

201807260566

- Symptom: In an ADCampus network, an automatically created aggregation group is deleted.
- Condition: This symptom occurs if only one of the aggregation group member ports is up.

201801050451

- Symptom: The MAC information of an 802.1X user is deleted. As a result, traffic cannot be forwarded.
- Condition: This symptom occurs if an 802.1X user logs in to the subordinate member device of an IRF fabric, and then the IRF fabric splits.

Resolved problems in R3208P15

201812060189

- Symptom: A user cannot log in to the switch through SSH when the number of online SSH users reaches 32.
- Condition: This symptom occurs if the device does not update the number of online SSH users after the SSH client logs out.

201812060193

- Symptom: The xmlcfgd process exits unexpectedly and a core file is created.
- Condition: This symptom occurs if the following operations have been performed:
  a. Bind more than 13 static addresses to the DHCP address pool.
  b. Use the SoapUI tool to perform a GET operation on the DHCP/DHCPServerPoolStatic table.

201812060181

- Symptom: The switch reboots unexpectedly after IPsec is configured.
- Condition: This symptom occurs if IPsec is configured.

201811130200

- Symptom: The port security process is locked.
- Condition: This symptom occurs if the following conditions exist:
  - The intrusion protection mode is disableport-temporarily on a port.
  - Port security triggers intrusion protection and sets the port to the down state while LLDP is obtaining user data from port security.

201811050088

- Symptom: The device is connected to an IMC server for portal authentication. The device is logged out because of security check failures.
- Condition: This symptom occurs if the device is connected to an IMC server and IMC is configured with a security policy to perform security check for the device.

201811140403

- Symptom:CVE-2018-15473

- Condition:OpenSSH is prone to a user-enumeration vulnerability. An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks. OpenSSH through 7.7 are vulnerable; other versions may also be affected.

201810110329

- Symptom: A 10-GE copper port cannot work at 10 Gbps or works unstably at 10 Gbps.
- Condition: This symptom occurs if the 10-GE copper port is directly connected to another 10-GE copper port.

201810110290

- Symptom: DHCP server MIBs fail to be read.
- Condition: None.

201809140102

- Symptom: Port security configuration changes after a software upgrade.
- Condition: This symptom might occur if the port security-configured switch is upgraded to R3208P10 or R3208P12.

201811300199

- Symptom: A portal user fails re-DHCP authentication, with a "Nonexistent username" error message prompted.
- Condition: This symptom might occur when a portal user performs re-DHCP authentication.

201811050128

- Symptom: Memory leaks occur to the service using the fast forwarding table.
- Condition: This symptom occurs if the following conditions exist:
  a. A large amount of traffic with varying quintuples is sent to the CPU through fast forwarding.
  b. The fast forwarding entries age out.

201810180032

- Symptom: When you enable BFD on an aggregate interface, the system prompts that the operation failed.
- Condition: This symptom occurs if the low bits of the source IP address and destination IP address are multicast addresses when you enable BFD on an aggregate interface.

201809050571

- Symptom: The controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued. When the display process command is executed, the output shows that a large number of residual configuration copy processes exist on the switch.
- Condition: This symptom might occur if the controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued.

201810120342

- Symptom: The switch cannot obtain the incoming and outgoing port numbers for traffic on an sFlow-enabled interface.
- Condition: This symptom might occur if sFlow is enabled on an interface.

201810150077

- Symptom: After a two-chassis IRF fabric reboots, MAC authentication users fail authentication on a port of the subordinate member.

- Condition: This symptom might occur if the IRF member devices each have a port that is working in the **userlogin-secure-or-mac** port security mode and MAC authentication users perform authentication on the port on the subordinate member after the IRF fabric reboots.

201809290352

- Symptom: A 10-gigabit fiber port has CRC packet error information after receiving traffic for a long period of time.
- Condition: This symptom might occur if a 10-gigabit fiber port has been receiving traffic for a long period of time.

201810300318

- Symptom: The CPU usage of the subordinate IRF member device becomes higher gradually.
- Condition: This symptom occurs if the IRF fabric runs for a long period of time and a large number of interface up/down events occur on the subordinate device.

201812170354

- Symptom: The **display device manuinfo** command does not display power supply information.
- Condition: This symptom occurs if the **display device manuinfo** command is executed.

Resolved problems in R3208P12

201808290664

- Symptom: In the **display dot1x** command output, the **Offline detect period** field is not aligned with the other fields.
- Condition: This symptom occurs if the **display dot1x** command is executed.

201809050749

- Symptom: Some deleted MAC address entries might remain.
- Condition: This symptom occurs if a large number of MAC address entries are learned and the **undo mac-address** command is used to delete MAC address entries.

201808090750

- Symptom: In QMC, ports on the device panel cannot be managed.
- Condition: This symptom occurs if QMC is used to manage the device.

201808160104

- Symptom: The MIB-Browser fails to read information of the DHCP server MIB nodes.
- Condition: This symptom occurs if the MIB-Browser is used to read information of the DHCP server MIB nodes.

201809050679

- Symptom: The local mirroring configuration does not take effect after the device is rebooted.
- Condition: This symptom occurs if STP is configured globally, local mirroring is configured, and then the device is rebooted.

201807310087

- Symptom: HTTPS redirection fails.
- Condition: This symptom occurs if HTTPS redirection is enabled and a user uses the browser in the MAC OS to access the server.

201806050164

- Symptom: The configuration of a Layer 3 aggregate interface is lost.
- Condition: This symptom occurs if a Layer 3 aggregate interface is configured, the configuration is saved, and the device is rebooted.

201808140119

- Symptom: The ACL function does not take effect.
- Condition: This symptom occurs if 802.1X issues authorization ACLs.

201808070167

- Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. An interface is configured with both MAC authentication and Web authentication.
  b. A user fails to pass MAC authentication.

201808060785

- Symptom: An 802.1X authentication server fails to issue authorization ACLs.
- Condition: This symptom occurs if 802.1X authentication is enabled and the authentication server issues authorization ACLs containing rules related to TCP or UDP services and port numbers to users.

201807210046

- Symptom: After a user logs in to the device by using SSH and then goes offline, remaining information of the user exists on the device.
- Condition: This symptom occurs if the user logs in to the device and then goes offline by using SSH frequently.

201807120164

- Symptom: Some UDP packets with the destination port number 6784 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on an IRF fabric.
  b. The IRF fabric receives UDP packets with the destination port number 6784.

201804260662

- Symptom: The following problems occur:
  - When a user performs authentication through HWTACACS, the user cannot successfully log in, and no debugging information is printed.
  - When a user performs authentication through RADIUS, the user can successfully log in, but part of the debugging information is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the AAA authentication method as HWTACACS or RADIUS.
  b. A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

201806120588

- Symptom: The panel of the device is not completely displayed on the Web interface.
- Condition: This symptom occurs if you log in to the Web interface of a device that has combo interfaces, and enter the **Dashboard** > **System Utilization** > **View Details** page.

201807160406

- Symptom: The MAC address entry aging timer is different from the offline detect timer.

- Condition: This symptom occurs if the hit bit of the first packet with the specified MAC address is not set during MAC authentication.

201806290399

- Symptom: The value of the snmpEngineboot node is incorrect.
- Condition: This symptom occurs if the whole IRF fabric is rebooted to cause a master/subordinate switchover.

201807160277

- Symptom: The RPS LED is off when the device is connected to an RPS.
- Condition: This symptom occurs when the device is connected to an RPS.

201807040644

- Symptom: PBR does not take effect on ports in a super VLAN.
- Condition: This symptom occurs if PBR is configured on a super VLAN interface.

201807040637

- Symptom: When the spanning tree protocol is disabled globally, spanning tree protocol packets cannot be flooded.
- Condition: This symptom occurs if the spanning tree protocol is disabled globally.

201807040593

- Symptom: After you modify the login password on the Web interface, you will fail to log in to the device again. In this case, you must set the password again.
- Condition: This symptom occurs if you log in to the device through the Web interface and modify the login password.

Resolved problems in R3208P10

201807190555

- Symptom: The NMS memory leaks.
- Condition: This symptom occurs if the **undo snmp-agent trap enable** command is used to disable SNMP notifications and the NMS walks on the SYSLOG-MSG-MIB node information.

201808020501

- Symptom: The device fails to obtain the authorization VLAN name in the \000xxxxx\000 format from the RADIUS server.
- Condition: This symptom might occur if the RADIUS server issues an authorization VLAN name in the \000xxxxx\000 format to an authenticated user.

201807310087

- Symptom: HTTPS redirection fails.
- Condition: This symptom occurs if HTTPS redirection is enabled and a user uses the browser in the MAC OS to access the server.

201806050164

- Symptom: The configuration of a Layer 3 aggregate interface is lost.
- Condition: This symptom occurs if a Layer 3 aggregate interface is configured, the configuration is saved, and the device is rebooted.

201808140119

- Symptom: The ACL function does not take effect.
- Condition: This symptom occurs if 802.1X issues authorization ACLs.

201808070167

- Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. An interface is configured with both MAC authentication and Web authentication.
  b. A user fails to pass MAC authentication.

201808060785

- Symptom: An 802.1X authentication server fails to issue authorization ACLs.
- Condition: This symptom occurs if 802.1X authentication is enabled and the authentication server issues authorization ACLs containing rules related to TCP or UDP services and port numbers to users.

201807210046

- Symptom: After a user logs in to the device by using SSH and then goes offline, remaining information of the user exists on the device.
- Condition: This symptom occurs if the user logs in to the device and then goes offline by using SSH frequently.

201807120164

- Symptom: Some UDP packets with the destination port number 6784 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on an IRF fabric.
  b. The IRF fabric receives UDP packets with the destination port number 6784.

201804260662

- Symptom: The following problems occur:
  - When a user performs authentication through HWTACACS, the user cannot successfully log in, and no debugging information is printed.
  - When a user performs authentication through RADIUS, the user can successfully log in, but part of the debugging information is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the AAA authentication method as HWTACACS or RADIUS.
  b. A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

201807160406

- Symptom: The MAC address entry aging timer is different from the offline detect timer.
- Condition: This symptom occurs if the hit bit of the first packet with the specified MAC address is not set during MAC authentication.

201806290399

- Symptom: The value of the snmpEngineboot node is incorrect.
- Condition: This symptom occurs if the whole IRF fabric is rebooted to cause a master/subordinate switchover.

201807160277

- Symptom: The RPS LED is off when the device is connected to an RPS.

- Condition: This symptom occurs when the device is connected to an RPS.

201807040644

- Symptom: PBR does not take effect on ports in a super VLAN.
- Condition: This symptom occurs if PBR is configured on a super VLAN interface.

201807040637

- Symptom: When the spanning tree protocol is disabled globally, spanning tree protocol packets cannot be flooded.
- Condition: This symptom occurs if the spanning tree protocol is disabled globally.

201807040593

- Symptom: After you modify the login password on the Web interface, you will fail to log in to the device again. In this case, you must set the password again.
- Condition: This symptom occurs if you log in to the device through the Web interface and modify the login password.

Resolved problems in R3208P08

201805250708

- Symptom: CVE-2016-9586
- Condition: Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

201804260567

- Symptom: NMS receives traps more than 10 minutes after the device reboots.
- Condition: This symptom occurs if the security model of SNMPv3 is authentication with privacy and the SNMP agent device is rebooted.

201806110087

- Symptom: The device might not respond when the **display ike sa** command is executed.
- Condition: This symptom occurs if the device acts as the IKE responder, and IKE SAs are established again after old IKE SAs are aged and deleted.

201804260604

- Symptom: IPsec tunnels are interrupted irregularly.
- Condition: This symptom occurs if IPsec are configured on two devices and the two devices initiate negotiation packets to each other at the same time.

201711290750

- Symptom: The SNMP function fails.
- Condition: This symptom occurs if the **snmp-agent port** command is used to modify the UDP port for receiving SNMP packets.

201806050863

- Symptom: The command execution result is not displayed.
- Condition: This symptom occurs if you enter the Python shell and execute Comware V7 commands.

201805290211

- Symptom: An access device cannot ping the core device.

- Condition: This symptom occurs if the following operations are performed:
  a. Two devices form an IRF fabric. The IRF fabric is connected to the core device through a multichassis aggregate link.
  b. The access device connects to the IRF fabric through an aggregate interface, and the aggregate interface is assigned to a port isolation group.
  c. Reboot the IRF fabric.

201806140516

- Symptom: ARP replies are dropped.
- Condition: This symptom occurs if a trunk port of the device sends ARP replies shorter than 64 bytes.

201806200110

- Symptom: The system does not automatically modify the QoS priorities for traffic in a voice VLAN.
- Condition: This symptom occurs if an interface has voice VLAN enabled and receives voice traffic.

201805250467

- Symptom: An interface on the device leaves the voice VLAN and cannot join the voice VLAN again.
- Condition: This symptom occurs if the following operations are performed:
  a. In an IRF fabric, an interface on a subordinate member device has LLDP enabled and voice VLAN configured, and is connected to a LLDP/CDP-capable voice device.
  b. Establish or disconnect LLDP neighbor relationship on the subordinate member device.

201805220359

- Symptom: The device continuously sends ARP requests.
- Condition: This symptom occurs if the following operations are performed:
  a. The device is configured with multiport ARP entries.
  b. Outgoing interface consistency check for ARP entries and MAC address entries is enabled.

201805250699

- Symptom: A device port learns the source MAC address in LLDP packets.
- Condition: This symptom occurs if the device port receives LLDP packets.

201802010506

- Symptom: An IP address cannot be configured for the device.
- Condition: This symptom occurs if an IRF member device is powered off and rebooted multiple times to perform master/subordinate switchovers.

201804090636

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  a. The network has a large number of short TCP connections.
  b. The device keeps receiving and sending packets.
  c. The device accesses resources that have been released by itself.

201802010690

- Symptom: The device discards packets with a checksum of 01 00.
- Condition: This symptom might occur if the checksum of incoming packets is 01 00.

201711160780

- Symptom: The energy saving configuration on a combo interface gets lost after the active port of the combo interface changes from the copper port to the fiber port and then back to the copper port.
- Condition: This symptom might occur if the following operations are performed:
  a. When the copper port of the combo interface is active, enable EEE and auto power-down on the combo interface.
  b. Activate the fiber port of the combo interface.
  c. When the fiber port of the combo interface is active, activate the copper port of the combo interface.

201805090571

- Symptom: When dropping unknown multicast data packets is enabled for a VLAN, the device floods multicast packets with TTL 0 in the VLAN.
- Condition: This symptom might occur if dropping unknown multicast data packets is enabled for the VLAN.

201804270451

- Symptom: An interface sends incoming ARP requests back to the source interfaces.
- Condition: This symptom might occur after the following operations are performed:
  a. Configure the interface as an ARP trusted interface by using the **arp detection trust** command.
  b. Assign the interface to an aggregation group.
  c. Delete the aggregation group or remove the interface from the aggregation group.

201804180241

- Symptom: The outgoing interface information is inconsistent in the MAC address entry and the ARP entry for the same MAC address.
- Condition: This symptom might occur if the MAC address moves frequently.

201805180576

- Symptom: Symptom: Non-first fragments of an IP packet, which do not contain TCP or UDP port numbers, match an ACL rule specified with TCP or UDP port numbers.
- Condition: This symptom might occur if the ACL rule is specified with TCP or UDP port numbers.

201801190229

- Symptom: CVE-2017-15896
- Condition: An attacker can exploit this issue to bypass TLS validate and encrypt, send application data to Node.js.

201801190229

- Symptom: CVE-2017-3737
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201801190229

- Symptom: CVE-2017-3738
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201705310258

- Symptom: The device reboots exceptionally at a very low probability.
- Condition: This symptom occurs if the device has been running for a long period of time and invalid memory is accessed when PBR determines whether the next hop is valid through querying the FIB table.

201706300315

- Symptom: When the status of a track entry associated with a static route changes, the static route does not respond to the change, and status of the static route's next hop does not change.
- Condition: This symptom occurs if a static route fails to establish a connection to the track module when the static route is associated with a track entry.

201804090334

- Symptom: It takes 20 seconds to log in to the device through SSH.
- Condition: This symptom occurs if you log in to the device through SSH after the password control feature is enabled.

201705310354

- Symptom: The rawip socket remains, which exhausts the memory and causes the device to reboot.
- Condition: This symptom occurs if you keep performing NQA operation for a period of time.

201706300478

- Symptom: The device cannot send ICMP error packets.
- Condition: This symptom occurs if the following conditions exist:
  - The **ip unreachables enable** and **ip ttl-expires enable** commands are configured on the device.
  - The device receives ICMP request packets.

201801290865

- Symptom: The prefix obtained from an IPv6 address is still advertised in RA messages.
- Condition: This symptom occurs if an IPv6 address is manually configured and then the **ipv6 nd ra prefix default no-advertise** command is configured to disable the device from advertising the prefix of the IPv6 address.

201802070015

- Symptom: The PoE function of interfaces still supplies power.
- Condition: This symptom occurs if PoE is disabled on all interfaces and then PoE is disabled on the PSE.

201801300024

- Symptom: Some BSR packets are dropped in a VLAN with IGMP snooping enabled.
- Condition: This symptom occurs if IGMP snooping is enabled for a VLAN and BSR packets are received at wire speed in the VLAN.

201803260509

- Symptom: The **bpdu-drop any** command configuration does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  a. On an IRF fabric, configure BFD MAD. Execute the **bpdu-drop any** command on the IRF physical interfaces.
  b. In system view, execute the **undo stp global enable/stp global enable** or **reboot** command. The STP status of interfaces changes.

201803160619

- Symptom: With MAC authentication enabled, the device does not disconnect a user and still displays the user as online when the device does not receive any packets from the user within the offline detection timer but the MAC address entry has not aged out.
- Condition: This symptom occurs if MAC authentication offline detection is enabled and the offline detection timer is different from the MAC address aging timer.

201803200427

- Symptom: Traps are received more than 10 minutes after the device is rebooted.
- Condition: This symptom occurs if the device is rebooted when authentication with privacy is configured for SNMPv3.

201802010956

- Symptom: The connection between an IRF fabric and a controller flaps.
- Condition: This symptom occurs if the following conditions exist:
  - OpenFlow devices form an IRF fabric.
  - A subordinate member device connects to the controller.
  - The subordinate member device receives 150-byte PIM packets at wire speed.

201801300586

- Symptom: An OpenFlow device is disconnected from the controller.
- Condition: This symptom occurs if the controller issues the **openflow shutdown** or **undo openflow shutdown** command twice.

201803230514

- Symptom: After a device configured with port security is rebooted, users fail to come online through MAC authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable port security, and set the port security mode to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt on an interface.
  b. Save the configuration, and delete the .mdb configuration file.
  c. Reboot the device.

201708150559

- Symptom: Dynamic MAC-based VLAN assignment is enabled on an interface, and the PVID of the interface is a secondary VLAN of a primary VLAN. If an incoming frame is tagged with the PVID and fuzzy MAC-to-VLAN entry match succeeds for the frame's source MAC address, the interface cannot forward the frame.
- Condition: This symptom might occur if the interface receives a frame that carries a VLAN ID same as the PVID of the interface, and the PVID is a secondary VLAN of a primary VLAN.

201712220061

- Symptom: CVE-2017-3736
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201712190289

- Symptom: CVE-2017-12190

- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

201712190289

- Symptom: CVE-2017-12192
- Condition: Attackers can exploit this issue to cause denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

201712190289

- Symptom: CVE-2017-15274
- Condition: An attacker can exploit this issue to cause a local denial-of-service condition.

201712190289

- Symptom: CVE-2017-15299
- Condition: An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.

201801190481

- Symptom: On an OpenFlow-enabled IRF fabric that contains two member switches, the **openflow shutdown** command is executed on an interface of the subordinate switch, and then the interface is brought up from the controller. After a master/subordinate switchover, status of an interface is abnormal on the new master.
- Condition: This symptom might occur if a master/subordinate switchover occurs after an interface that has been shut down by OpenFlow on the subordinate switch is brought up from the controller.

201801180979

- Symptom: When receiving PIM bootstrap messages with a length of 1500 bytes, the switch can send only five bootstrap messages per second in a VLAN enabled with IGMP snooping.
- Condition: This symptom might occur if IGMP snooping is enabled for a VLAN.

201712230037

- Symptom: When the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface, the switch forwards the packet by using an incorrect route.
- Condition: This symptom might occur if the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface.

201801040748

- Symptom: ACLs are not completely deleted from the hardware after IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.
- Condition: This symptom might occur if IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.

201801180968

- Symptom: The switch is connected to a VRRP group. After the link between the VRRP master and the switch flaps, the switch has an incorrect ARP entry for the VRRP master.
- Condition: This symptom might occur if the switch is connected to a VRRP group, and the link between the VRRP master and the switch flaps.

201711290635

- Symptom: When a port joins a Layer 2 aggregation group, the allowed jumbo frame length configured on the Layer 2 aggregate interface is not synchronized to that port.

- Condition: This symptom might occur if a port joins a Layer 2 aggregation group that is configured with the allowed jumbo frame length setting.

201712210545

- Symptom: In the output from the **display transceiver diagnosis interface** command, the receive power of transceiver modules is incorrect.
- Condition: This symptom might occur if the **display transceiver diagnosis interface** command is executed.

201806040605

- Symptom: The status of the LED for an interface is incorrect.
- Condition: This symptom occurs if EEE is enabled on the interface and the interface is up.

Resolved problems in R3208P03

201711030370

- Symptom: CVE-2017-1000253
- Condition: Local attackers may exploit this issue to gain root privileges.

201711230489

- Symptom: The device reboots unexpectedly when reading an Entity MIB node.
- Condition: This symptom might occur if the device reads an Entity MIB node.

201711230366

- Symptom: The device reboots unexpectedly after receiving a packet-out message without the output or group action issued by the controller.
- Condition: This symptom might occur if the device receives a packet-out message without the output or group action issued by the controller.

201711230694

- Symptom: The device might fail to delete the configurations of HWTACACS servers when the configurations of HWTACACS servers are frequently deleted. Or, a process exception might occur if the device rolls back the configuration.
- Condition: This symptom might occur if the following conditions exist:
  - The HWTACACS scheme configured on the device contains configurations of multiple HWTACACS authentication, authorization, and accounting servers.
  - The HWTACACS authentication, authorization, or accounting servers have the same VPN instance and IP address settings but different port numbers.

201712040081

- Symptom: In an IRF fabric, the console port on the subordinate device hangs and some information of the subordinate device cannot be viewed on the master device.
- Condition: This symptom might occur if the following conditions exist:
  - The IRF fabric is configured with the spanning tree feature.
  - The peer switch is disabled with the spanning tree feature.
  - A loop exists between the IRF fabric and the peer switch.

201711280600

- Symptom: After certain operations are performed, the **display mac-address** command does not display the voice VLAN MAC address entry of an IP phone. When the settings on the

interface connected to the IP phone are removed and reconfigured, the IP phone cannot join a voice VLAN.

- Condition: This symptom might occur if the following operations are performed:
  a. Connect an IP phone to an interface.
  b. Configure voice VLAN and port security on the interface.
  c. Remove the settings from the interface and reconfigure them on the interface.

201711280538

- Symptom: MAC address entries of MAC authentication users do not age out after the users go offline.
- Condition: This symptom might occur if the following conditions exist:
  - A Layer 2 switch configured with the spanning tree feature exists between the device and the authentication clients.
  - The device is enabled with MAC authentication.
  - The aging timer for dynamic MAC address entries is set to a value greater than 60 seconds by using the **mac-address timer aging** *seconds* command.

201710300395

- Symptom: A remark action conflict is prompted when a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.
- Condition: This symptom might occur if a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.
-

201711110038

- Symptom: A user fails 802.1X or MAC authentication when the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides
- Condition: This symptom might occur if the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides.

201709250409

- Symptom: The mirroring and STP settings are partially lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Delete some SNMP settings.
  b. Save the configuration by using the **save force** command and reboot the device.

201708280341

- Symptom: MAC authentication fails after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security, and set the port security mode to **userlogin-secure-or-mac** on an interface.
  b. Save the configuration and upgrade the software, or reboot the switch and use a .cfg file to restore the configuration.

201708280275

- Symptom: An 802.1X user that passes authentication on an interface is assigned an IP address in the guest VLAN, Auth-Fail VLAN, or critical VLAN instead of an IP address in the authorization VLAN.
- Condition: This symptom might occur if the following conditions exist:

- Both 802.1X and DHCP are enabled.
- An 802.1X guest VLAN, Auth-Fail VLAN, or critical VLAN is configured on the interface.
- The server successfully assigns an authorization VLAN.

201708280259

- Symptom: 802.1X authentication fails on an interface.
- Condition: This symptom might occur if the following operations are performed:
  - Enable 802.1X and specify the port-based access control method on an interface.
  - Set the username request timeout timer by using the **dot1x timer tx-period** *tx-period-value* command.

201708280255

- Symptom: A user logs in to the CLI through a console port. The CLI hangs up after the user executes the **stp edged-port** and **stp loop-protection** commands in interface range view.
- Condition: This symptom might occur if AAA authentication is enabled for CLI login by using the **authentication-mode scheme** command and command accounting is enabled by using the **command accounting** command.

201710300047

- Symptom: The **snmp-agent target-host trap** command configuration is lost after a master/subordinate switchover is performed in an IRF fabric.
- Condition: This symptom occurs if the *vpn-instance-name* or *security-string* argument in the command contains dots (.).

201708280230

- Symptom: A user passes MAC authentication on an interface with port security configured after failing 802.1X authentication. The user fails MAC authentication after the **shutdown** and **undo shutdown** commands are executed on the interface.
- Condition: This symptom occurs if the port security mode is set to **userlogin-secure-or-mac-ext** on the interface.

201710260388

- Symptom: The device does not support the ACL deployed by the 802.1X authentication server.
- Condition: This symptom occurs if a rule in the deployed ACL contains the range keyword.

201709250739

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201710200010

- Symptom: Automatic configuration fails because a VLAN interface cannot obtain an IP address.
- Condition: This symptom occurs when the device starts up without a configuration file.

201708310208

- Symptom: Web authentication entries exist, and users of other authentication types fail authentication or fail to get authorized when a large number of users exist.
- Condition: This symptom might occur if the following operations are performed when Web authentication is disabled:
  a. Configure the **web-auth free-ip** command.
  b. Reboot the device.

201710310028

- Symptom: In an IRF fabric, the RRPP convergence time is 6 to 10 seconds after a master/subordinate switchover is performed upon a master reboot.
- Condition: This symptom occurs if two RRPP domains are configured on the IRF fabric.

201710260631

- Symptom: A 10 GE copper interface cannot come up.
- Condition: None.

201710270144

- Symptom: The device fails to automatically execute the **save force** command.
- Condition: This symptom might occur if the **save force** command is added to the autocfg configuration file.

201708310228

- Symptom: Packet filtering does not work after the switch is rebooted.
- Condition: This symptom might occur if the switch is rebooted after packet filtering is configured.

201709220068

- Symptom: On an IRF fabric, the view of some interfaces might be unavailable after an IRF master/subordinate switchover.
- Condition: This symptom might occur if an IRF master/subordinate switchover occurs when a new member joins the IRF fabric.

201709040292

- Symptom: With the HWTACACS accounting server being blocked, the switch responds slowly to commands input by a Telnet user.
- Condition: This symptom might occur if HWTACACS authentication is enabled for login.

201710270540

- Symptom: Certain QoS policies cannot be applied.
- Condition: This symptom might occur if one of the following operations are performed.
  - Apply a QoS policy that matches the outer VLAN IDs or inner VLAN IDs to the inbound direction of an interface for outer VLAN ID remarking.
  - Apply a QoS policy that matches the inner VLAN IDs to the inbound direction of an interface for inner VLAN ID remarking.
  - Apply a QoS policy that matches the outer VLAN IDs to the outbound direction of an interface for inner VLAN ID remarking.

201710200099

- Symptom: sFlow cannot collect outgoing traffic statistics on an interface.
- Condition: This symptom might occur if sFlow is configured on an interface.

201709010571

- Symptom: LLDP is enabled globally and on an interface. The LLDPDUs sent by the interface show that autonegotiation is supported and enabled, but the PMD parameter Auto-negotiated Advertised Capability field is all zeros.
- Condition: This symptom might occur if LLDP is enabled globally and on an interface.

Resolved problems in R3208

201704280459

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201704280459

- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

201704270120

- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201707200766

- Symptom: During automatic ADCampus deployment, the switch does not replace the configuration on a downlink interface with the trunk port configuration when an AP accesses the switch through the downlink interface.
- Condition: This symptom might occur if the switch acts as an access node on the ADCampus network.

2016707110001

- Symptom: A terminal connected to an interface enabled with EEE cannot ping the switch.
- Condition: This symptom might occur if the terminal connects to the switch through an interface enabled with EEE.

Resolved problems in R3207

None

Resolved problems in R3115P08

201703060242

- Symptom: Packet loss occurs on an edge aggregate interface if the interface has not received LACPDUs within the LACP timeout interval.
- Condition: This symptom might occur if an edge aggregate interface has not received LACPDUs within the LACP timeout interval.

201703060053

- Symptom: The switch is connected to a Cisco IP phone installed with a key expansion module. When PoE is enabled on the interface connected to the phone, the phone can be powered on, but the key expansion module cannot start.

- Condition: This symptom might occur if the following operations are performed:
  a. Connect the switch to a Cisco IP phone installed with a key expansion module.
  b. Enable PoE on the interface connected to the phone.
  c. Set the maximum power for the PoE-enabled interface.

201508120317

- Symptom: The switch uses a software version earlier than R3109P09, and PoE and LLDP are bled on an interface. When the interface flaps, the switch irregularly generates the CFGMAN_CFGCHANGED message to report configuration changes.
- Condition: This symptom might occur if the following conditions exist:
  - The switch uses a software version earlier than R3109P09.
  - PoE and LLDP are enabled on an interface, and the interface flaps.

201607280306

- Symptom: SSH connections cannot be established if no Suite B cryptographic suite is specified for SSH.
- Condition: This symptom might occur if no Suite B cryptographic suite is specified for SSH.

201606130301

- Symptom: An authentication server cannot be removed from a TACACS scheme in the Web interface.
- Condition: This symptom might occur if an authentication server is removed from a TACACS scheme in the Web interface.

201606080536

- Symptom: An AudioCodes IP phone sending CDP packets cannot be assigned to the critical voice VLAN.
- Condition: This symptom might occur if an AudioCodes IP phone sends CDP packets.

Resolved problems in R3115P07

201701170366

- Symptom: The user VLAN information in user event logs is inconsistent with the authorization VLAN information that the server issues to users.
- Condition: This symptom might occur if the server issues authorization VLAN information to users that pass authentication.

201701040586

- Symptom: The **display vlan brief** command cannot display information about VLANs numbered the multiple of 41.
- Condition: This symptom might occur if the number of VLANs on the switch reaches the upper limit.

201611220420

- Symptom: The console port of an IRF master might be inaccessible.
- Condition: This symptom might occur if the tty and comsh processes run on different CPU cores.

201611110196

- Symptom: In certain conditions, the **display stp brief** command displays incorrect status information for a port.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable STP on the switch and its peer device.
  b. Enable loop detection on the port connected to the peer device, and disable STP on the peer device.
  c. Execute the display stp brief command for the port.

201702060403

- Symptom: The 5130-24G-2SFP+-2XGT EI JG938A/5130-48G-2SFP+-2XGT EI JG939A/130-24G-PoE+-2SFP+-2XGT (370W) EI JG940A/5130-48G-PoE+-2SFP+-2XGT (370W) EI JG941A switch might lose software image files and configuration files.
- Condition: None.

201702130126

- Symptom: In certain conditions, an IRF fabric cannot be pinged after it reboots.
- Condition: This symptom might occur if port security is enabled on the IRF fabric, and the maximum number of secure MAC addresses allowed on a port is set to 1.

201701190157

- Symptom: In certain conditions, users cannot come online after the IRF fabric that the users access is rebooted.
- Condition: This symptom might occur if the following conditions exist:
  - Port security is enabled on the IRF fabric, and port security in **userlogin-secure** mode is enabled on the port that the users access.
  - The IRF fabric is rebooted.

201702090546/201701100036

- Symptom: After an IRF fabric is rebooted, some subordinate switches fail to respond, and the CLI of these switches is inaccessible. Output from the **display device** command shows that these switches are in Fault state.
- Condition: This symptom might occur if the following conditions exist:
  a. The IRF fabric contains dual-chip switches.
  b. The IRF fabric is rebooted.

201701180065

- Symptom: Multicast traffic fails to be forwarded out of an aggregate interface.
- Condition: This symptom occurs if the status of one member port in the aggregation group changes from Unselected to Selected after the device learns multicast routes. The aggregate interface is an outgoing interface of one of the multicast routes.

201701170120

- Symptom: A memory leakage occurs on the device.
- Condition: This symptom occurs if MFF in the automatic mode is enabled and then disabled repeatedly.

201701060282

- Symptom: The device generates the log message "**RESEND_RADIUS:Failed to allocate PktID**".

- Condition: This symptom occurs if a large number of users come online and go offline frequently when the primary RADIUS accounting server and secondary RADIUS accounting servers are unreachable.

Resolved problems in R3115P06

201611090264

- Symptom: An SFTP user assigned the network-operator user role has access to some commands that are supposed to be inaccessible to the user role.
- Condition: This symptom occurs if the SFTP user passes either publickey or password-publickey authentication to log in to the device and is assigned the network-operator user role.

201611070270

- Symptom: CVE-2016-8858
- Condition: A remote user can send specially crafted data during the key exchange process to trigger a flaw in kex_input_kexinit() and consume excessive memory on the target system. This can be exploited to consume up to 384 MB per connection.

201609300342

- Symptom: A memory leakage occurs in the stpd process.
- Condition: This symptom occurs if the spanning tree feature is enabled on the device and the spanning tree operating mode is changed.

201611080056

- Symptom: CVE-2016-5195
- Condition: Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping.

201611220390

- Symptom: Authentication for new portal users fails when a large number of online portal users are logging out.
- Condition: This symptom might occur if the following conditions exist:
  - The RADIUS server provides accounting services for portal users.
  - A large number of online portal users log out.

201611220420

- Symptom: An IRF fabric cannot be accessed through the console port of the master.
- Condition: This symptom might occur if an IRF fabric is accessed through the console port of the master.

201611220435

- Symptom: After a two-chassis IRF fabric is rebooted, interface indexes change and Smart Link settings are lost.
- Condition: This symptom might occur if the following operations are performed:
  a. Delete the startup.mdb and ifindex.dat files on the IRF member switches.
  b. Save the configuration and reboot the IRF fabric.
  c. When the IRF member switches are rebooting, press Ctrl+B to access the Boot ROM menu of one IRF member switch. The other member switch is successfully rebooted.

201612080146

- Symptom: The switch stops responding when the scripts are executed to repeatedly display memory information about the ipoe and ifmgr processes.
- Condition: This symptom might occur if the scripts are executed to repeatedly display memory information about the ipoe and ifmgr processes.

201611220280

- Symptom: After an IRF fabric is rebooted, the VPN instance information on the master is incorrect.
- Condition: This symptom might occur if the following operations are performed on an IRF fabric:
  a. Create tunnel interfaces.
  b. Reboot the IRF fabric.

201612070648

- Symptom: 802.1X users fail 802.1X authentication.
- Condition: This symptom occurs if the primary RADIUS server frequently becomes unreachable and a large number of 802.1X users frequently come online and go offline.

201609120255

- Symptom: A large number of RXLOS interruptions occur on a transceiver module, which causes a high CPU usage and then causes the device to reboot.
- Condition: This symptom occurs if the device is connected to a port of a test device through the transceiver module.

201612090524

- Symptom: In log messages, the VLAN ID of a user is not the authorization VLAN ID assigned to the user.
- Condition: This symptom might occur if a user passes access authentication and is assigned to the authorization VLAN issued by the server.

201612080309

- Symptom: The NTP server sends the switch NTP packets that have the leap flag set to 01, but the local leap indicator of the switch is 00, and the leap flag of NTP packets sent by the switch is 00.
- Condition: This symptom might occur if the following conditions exist:
  a. A PC is directly connected to the switch's management interface and is configured as an NTP client.
  b. An NTP server sends the switch NTP packets with the leap flag set to 01.

201612060351

- Symptom: The dynamic MAC count is always displayed as 0.
- Condition: This symptom might occur if the **display openflow instance** command is used to display detailed information of an OpenFlow instance.

201612050429

- Symptom: Port isolation does not take effect. Traffic statistics exist on other aggregation group member ports.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure an aggregation group and configure port isolation on its member ports.
  b. Shut down all member ports by using the shutdown command or unplugging network cables.

c. Restore the member ports to the up state.

d. Send traffic to an aggregation group member port.

201611250474

- Symptom: The device adds two layers of VLAN tags to an untagged packet.
- Condition: This symptom might occur if the following conditions exist:
  a. Switch A and Switch B are directly connected through trunk ports. The trunk ports permit a VLAN.
  b. Configure an access port on Switch A and Switch B, and assign the access ports to the VLAN. Configure QinQ and L2PT on the access ports.
  c. Send untagged L2PT protocol packets to the access ports.

201611180294

- Symptom: A port goes down.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security on the port and configure the limit on the number of secure MAC addresses.
  b. Send packets according to the configured limit on the number of secure MAC addresses.

201611090199

- Symptom: The debugging information has extra spaces.
- Condition: This symptom might occur if the following operations are performed:
  a. A user logs in to the device by using SSH.
  b. The user enters incorrect passwords for three times.
  c. The user fails to log in and is added to the blacklist.
  d. The debugging information of the server is viewed.

201610150081

- Symptom: Some users pass the authentication, but the MAC addresses of these users are not learned.
- Condition: This symptom might occur if the following conditions exist:
  - Five devices form an IRF fabric, including four S5130-52S-EI switches and one S5130-28S-EI switch.
  - Import the user configuration and enable MAC authentication on all ports.
  - Use an auxiliary device to bring up all the devices and perform authentication. The authentication users on each device are the same. As a result, these users are frequently moved among different devices.
  - Send authentication traffic for a period of time. Then, stop authentication traffic on four devices, and leave authentication traffic on only one device.

201610260405

- Symptom: A user fails to log in to the device.
- Condition: This symptom might occur if the following conditions exist:
  a. The tcp syn-cookies enable command is executed.
  b. The Telnet client is not directly connected to the device.
  c. The user uses an IPv6 address to log in to the device by using SSH or Telnet.

201609230450

- Symptom: When a large number of IPv6 ND messages are learned and aged, traffic forwarding might fail because ARP/ND entries fail to be issued.

- Condition: This symptom might occur if a large number of IPv6 ND messages are learned and aged.

201607180428

- Symptom: IS-IS neighborship can be established. However, routing information cannot be obtained.
- Condition: This symptom might occur if the NX9000 device sends protocol packets with the MT IS TLV whose length is 2 bytes. HPE devices consider the length as invalid. As a result, the LSPs are considered as incorrect and dropped.

201603140259

- Symptom: The device operates improperly because the fast forwarding entries and sessions generated after tunnel encapsulation are incorrectly associated.
- Condition: This symptom might occur if the byte sequence is not converted for some fields in IP headers when fast forwarding entries and sessions are generated before tunnel encapsulation.

201610260040

- Symptom: The logbuffer cannot continue to record more logs.
- Condition: This symptom might occur if the following conditions exist:
  - The **info-center syslog min-age** command is not configured.
  - Adjust the system running time to be earlier than the system time.
  - The logbuffer is full.

201610260323

- Symptom: The system prompts that the characters fail to be input.
- Condition: This symptom might occur if you enter special characters when configuring a description on a client running the Windows 10 operating system.

201610260451

- Symptom: A user cannot use the correct username and password to log in to the device through the management interface or console interface.
- Condition: This symptom might occur if the **password-control enable** command is used to enable password control on the device and a large number of users use incorrect usernames and passwords to log in to the device.

201610140261

- Symptom: CVE-2016-6304
- Condition: Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

201610140261

- Symptom: CVE-2016-6306
- Condition: The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

201607280524

- Symptom: CVE-2016-2177
- Condition: OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.

201605090045

- Symptom: The unsupported QCN and DCBX options are configurable on the LLDP TLV configuration page of the Web interface.
- Condition: This symptom might occur if the following operations are performed:
  a. Access the device through the Web interface.
  b. On the Network > LLDP > LLDP-TLV page, select an interface, select 802.1TLVs QCN and DCBX, and apply the settings.

Resolved problems in R3115P05

201608170166

- Symptom: After the IMC server issues the class attribute to the NAS, the RADIUS accounting requests that the NAS sends to the server do not carry the class attribute.
- Condition: This symptom might occur if the IMC server issues the class attribute to the NAS after users pass RADIUS authentication.

201610090108

- Symptom: Two users who use the same MAC address exist on the switch when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  a. Both MAC authentication and 802.1X authentication are performed for the users, and MAC authentication is successful.
  b. MAC move is enabled on interfaces.

201609300434

- Symptom: On an IRF fabric, OUI addresses are lost after a master/subordinate switchover.
- Condition: This symptom might occur if the following conditions exist:
  a. The number of OUI addresses reaches the upper limit on the IRF fabric.
  b. A master/subordinate switchover occurs after the configuration is saved.

201609200500

- Symptom: The following symptoms might occur when a PBR policy is configured through the Web interface:
  - On the PBR configuration page, select **Match IPv4 ACL** to enter the ACL configuration page. A user stays on the ACL configuration page after the user adds an ACL successfully.
  - A user is redirected to the Web interface home page after the user adds a PBR policy that only has next hop information because the system does not check for empty fields for PBR policy configuration.
- Condition: This symptom might occur if a PBR policy is configured through the Web interface.

201609220002

- Symptom: In the help information of the **jumboframe enable** command, the maximum frame length is not 12000.
- Condition: This symptom might occur if the help information is displayed for the **jumboframe enable** command.

201609020107

- Symptom: When the EAD assistant redirect URL is configured through the Web interface, the system displays the "configuration already exists" message even if the configuration does not exist or take effect.

- Condition: This symptom might occur if the EAD assistant redirect URL is configured through the Web interface.

201607040335

- Symptom: A user cannot join the critical VLAN of MAC authentication when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  a. The user fails MAC authentication and is assigned to the guest VLAN.
  b. The authentication server becomes unavailable.
  c. The reset mac-authentication guest-vlan command is executed.

201606270081

- Symptom: The switch does not process EAPOL v3 packets of 802.1X authentication and displays the "Invalid protocol version ID" message.
- Condition: This symptom might occur if the switch receives EAPOL v3 packets of 802.1X authentication.

201603140511

- Symptom: When LLDP is disabled globally, the CPU usage of the LLDP process immediately increases to 20%-30%.
- Condition: This symptom might occur if LLDP is disabled globally.

201610150081

- Symptom: When certain conations exist, an IRF fabric does not have MAC address entries for users who pass MAC authentication. As a result, the users cannot access the network.
- Condition: This symptom might occur if the following conditions exist:
  - MAC authentication is enabled on all ports of the IRF fabric.
  - A large number of users move frequently, or ports go down and come up frequently.

Resolved problems in R3115P03

201607280521

- Symptom: CVE-2012-0036
- Condition: Fixed vulnerability in curl and libcurl 7.2x before 7.24.0 that allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.

201606280241

- Symptom: CVE-2016-4953
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.

201606280241

- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.

201606280241

- Symptom: CVE-2016-4956

- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

201608290241

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms.

201609060439

- Symptom: The operating status of BFD MAD for IRF is **Faulty**.
- Condition: This symptom occurs if BAD MAD is enabled for both the IRF fabric and the peer device and the IRF fabric receives BFD MAD packets from the peer device.

201607010063

- Symptom: Prompt messages occur in wrong order when the device decompresses a software image. The message that prompts users whether to delete the .ipe file appears before the message that prompts users to verify the legitimacy of the software image.
- Condition: This symptom occurs if the software of a member device is upgraded at the CLI by using the **boot-loader** command.

201609070269

- Symptom: PD detection and classification on a port are affected after PoE performs power negotiation on the port.
- Condition: None.

201608310495

- Symptom: The error message "Scanning is interrupted" occurs during ARP scanning.
- Condition: This symptom occurs if ARP scanning for secondary address ranges is configured after the device software is upgraded to R3109P03 or a later software version.

201608250027

- Symptom: The configuration of voice VLANs fails.
- Condition: This symptom occurs if voice VLANs are configured in batch in the Web interface.

201507220217

- Symptom: Maximum PI power negotiation fails on an interface configured with PoE.
- Condition: This symptom occurs if the maximum PI power is automatically deployed on the interface and the device is rebooted after the configuration is saved.

Resolved problems in R3115P01

201605050154

- First found-in version: 5130EI-CMW710-R3113P02
- Symptom: After the COA issues an authorization ACL, the session-timeout timer and the offline function do not operate correctly for the authentication users.
- Condition: This symptom occurs if the switch has MAC authentication or 802.1X authentication enabled.

201607190589

- Symptom: When a port enabled with 802.1X authentication is repeatedly shut down and brought up, the 802.1X client directly connected to the port is logged off for authorization failure.

- Condition: This symptom might occur if a port enabled with 802.1X authentication is repeatedly shut down and brought up, and an 802.1X client is directly connected to the port.

201605180172

- Symptom: The **undo speed auto downgrade** and **speed auto downgrade** commands are executed on all ports of the device, and the running configuration is saved. After a reboot, automatic negotiation for speed downgrading is not enabled on all ports.
- Condition: This symptom might occur if the following operations are performed:
- Execute the **undo speed auto downgrade** and **speed auto downgrade** commands on all ports.
- Save the running configuration and reboot the switch.

201604260394

- Symptom: The short LACP timeout interval (3 seconds) is set on member ports of an aggregate interface. When the aggregate interface is down, traffic interruption lasts for 3 seconds instead of 6 seconds.
- Condition: This symptom might occur if the short LACP timeout interval (3 seconds) is set on member ports of an aggregate interface.

201605090525

- Symptom: CVE-2015-8138
- Condition: Fixed vulnerability in ntpd which attackers may be able to disable time synchronization by sending a crafted NTP packet to the NTP client.

201605090525

- Symptom: CVE-2015-7979
- Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.

201605090525

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201605090525

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201605170547

- Symptom: CVE-2016-1550
- Condition: Fixed vulnerability in ntpd function allow an attacker to conduct a timing attack to compute the value of the valid authentication digest causing forged packets to be accepted by ntpd.

201605170547

- Symptom: CVE-2016-1551
- Condition: Fixed vulnerability in ntpd allows unauthenticated network attackers to spoof refclock packets to ntpd processes on systems that do not implement bogon filtering.

201605170547

- Symptom: CVE-2016-2519
- Condition: Fixed vulnerability in ntpd will abort if an attempt is made to read an oversized value.

201605170547

- Symptom: CVE-2016-1547
- Condition: Fixed vulnerability where an off-path attacker can deny service to ntpd clients by demobilizing preemptable associations using spoofed crypto-NAK packets.

201605170547

- Symptom: CVE-2016-1548
- Condition: Fixed vulnerability where an attacker can change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode.

201605170547

- Symptom: CVE-2015-7704
- Condition: Fixed vulnerability in ntpd that a remote attacker could use, to send a packet to an ntpd client that would increase the client's polling interval value, and effectively disable synchronization with the server.

Resolved problems in R3115

201605250614

- Symptom: The **speed auto a b** or **speed auto a b c** command is configured for an interface. After a reboot, only the **speed auto b** or **speed auto c** setting takes effect.
- Condition: his symptom might occur if the following operations are performed:
- Configure the **speed auto a b** or **speed auto a b c** command on the interface.
  a. Save the configuration.
  b. Reboot the device and use the .cfg configuration file to restore the configuration.

201606070566

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070566

- Symptom: CVE-2016-2106
- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070566

- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.02h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.

201606070566

- Symptom: CVE-2016-2108

- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).

201606070566

- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

201606070566

- Symptom: CVE-2016-2176
- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service

Resolved problems in R3113P05

201605030246

- Symptom: When a PC is quickly plugged and unplugged, the switch considers the PC as online.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has both MAC authentication and 802.1X authentication enabled.
  - The PC performs MAC authentication.
  - The interface connecting to the PC has the unicast trigger or MAC authentication delay function configured.

201606010228

- Symptom: An interface cannot correctly forward multicast packets.
- Condition: This symptom occurs if both 802.1X authentication and MAC authentication are enabled on the interface and a user successfully passes MAC authentication.

201605060393

- Symptom: After a master/subordinate switchover, the VLAN configurations of interfaces are lost.
- Condition: This symptom occurs if the IRF subordinate member switch is rebooted and a master/subordinate switchover is performed.

201605170504

- Symptom: In a three-chassis IRF fabric, after the master member is powered off and subordinate member 1 becomes the new master member, the VLAN configurations of interfaces on subordinate member 2 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use three switches to build an IRF fabric in a daisy-chain topology.
  b. Power on the master member.
  c. Power on subordinate member 1 and then subordinate member 2.
  d. Save the configuration after the IRF fabric is formed.

201601090054

- Symptom: When TCP port X is enabled, TCP port X + 2048*N is also enabled (N is an arbitrary integer).

- Condition: This symptom occurs if TCP port X is enabled, for example, TCP port 23 is enabled by using the **telnet server enable** command.

201603100197

- Symptom: On an inactivity aging-enabled interface, sticky MAC addresses age out before the secure MAC aging timer set by using the **port-security timer autolearn aging** command expires.
- Condition: This symptom might occur if the following operations are performed on an interface:
  - Enable port security and inactivity aging.
  - Use the **port-security timer autolearn aging** command to set the secure MAC aging timer.

Resolved problems in R3113P03

201604091715

- Symptom: When a 10G Base-T port is connected to a specific device model, speed autonegotiation takes 20 to 30 seconds and the negotiation result can only be 1 Gbps.
- Condition: This symptom might occur if a 10G Base-T port is connected to a specific device model.

Resolved problems in R3113P02

201604110101

- Symptom: After a period of time, PCs cannot join the 802.1X guest VLAN.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has both 802.1X authentication and MAC authentication enabled.
  - The switch connects to multiple PCs through a hub.
  - The PCs fail to pass the MAC authentication.

201605180172

- Symptom: After the switch is rebooted, the speed downgrading autonegotiation configuration is undo speed auto downgrade on an interface that is configured with the speed auto downgrade command.
- Condition: This symptom occurs if the following operations are performed

201602010060

- Symptom: After the configuration of an IRF fabric is restored by using .cfg files, RIP route filtering configuration is lost.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable RIP on an IRF fabric.
  b. Configure the filter-policy import or filter-policy export command for an interface on a subordinate switch.
  c. Restore the configuration of the IRF fabric by using .cfg files.

201603010580

- Symptom: The VLAN dropdown list is unavailable on the **Network** > **IPv6** > **ND** > **New Neighbor Entry** page of the Web interface.
- Condition: This symptom might occur if IPv6 neighbor entries are configured on the **Network** > **IPv6** > **ND** > **New Neighbor Entry** page of the Web interface.

201508190171

- Symptom: After the MAC address entry and ARP entry of a MAC authentication user age out, the switch cannot generate new MAC address entry and ARP entry for the user.
- Condition: This symptom might occur if the following conditions exist:
  - MAC authentication is enabled, and MAC authentication offline detection is disabled.
  - The MAC address entry and ARP entry of a MAC authentication user age out.

201507300295

- Symptom: When DHCP snooping is enabled on an IRF fabric using the ring topology, IRF member switches reboot repeatedly.
- Condition: This symptom might occur if DHCP snooping is enabled on an IRF fabric using the ring topology.

201604140100

- Symptom: MAC authentication users cannot come online if the server issues the Cisco-AVPair attribute to the switch.
- Condition: This symptom might occur if the server issues the Cisco-AVPair attribute to the switch.

201603120042

- Symptom: The switch does not respond to the security commands input by a console user.
- Condition: This symptom might occur if the following conditions exist:
  - LLDP and access authentication are enabled on the switch.
  - The intrusion protection action is set to disable on an interface, and intrusion protection is triggered because the phone connected to the interface fails authentication.

201603230420

- Symptom: CVE-2016-0705
- Condition: Fixed vulnerability when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources.

201603230420

- Symptom: CVE-2016-0798
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt.

201603230420

- Symptom: CVE-2016-0797
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference).

201603230420

- Symptom: CVE-2016-0799
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service which could lead to memory allocation failure or memory leaks.

201603230420

- Symptom: CVE-2016-0702

- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g which makes it easier for local users to discover RSA keys leveraging cache-bank conflicts, aka a "CacheBleed" attack.

201603230420

- Symptom: CVE-2016-2842
- Condition: Fixed vulnerability in the doapr_outch function in crypto/bio/b_print.c, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string.

201603170138

- Symptom: CVE-2016-0701
- Condition: Fixed vulnerability in the DH_check_pub_key function which makes it easier for remote attackers to discover a private DH (Diffie-Hellman) exponent by making multiple handshakes with a peer that chose an inappropriate number. This issue affects OpenSSL version 1.0.2. and addressed in 1.0.2f. OpenSSL 1.0.1 is not affected by this CVE.

201603170138

- Symptom: CVE-2015-3197
- Condition: Fixed vulnerability when using SSLv2 which can be exploited in a man-in-the-middle attack, if device has disabled ciphers.

201512280388

- Symptom: 802.1X users are reauthenticated.
- Condition: This symptom occurs if the following conditions exist:
  - The keep-online feature is enabled for 802.1X users.
  - Online 802.1X users receive EAPOL-Start packets.

201602040568

- Symptom: An IP phone is reauthenticated every 30 seconds when the Web authentication server is unreachable.
- Condition: This symptom occurs if the IP phone is connected to a port enabled with 802.1X authentication and Web authentication.

201602160644

- Symptom: The ARP packets received from a peer device are not broadcasted in a VLAN.
- Condition: This symptom occurs if ARP snooping is enabled in the VLAN.

201510150328

- Symptom: The **undo ssl version** { **tls1.0** | **tls1.1** } **disable** command configuration does not take effect.
- Condition: This symptom occurs if the switch is operating in FIPS mode or non-FIPS mode.

201512290192

- Symptom: CVE-2015-3194
- Condition: Fixed vulnerability which can be exploited in a DoS attack, if device is presented with a specific ASN.1 signature using the RSA.

201512290192

- Symptom: CVE-2015-3195
- Condition: Fixed vulnerability with malformed OpenSSL X509_ATTRIBUTE structure used by the PKCS#7 and CMS routines which may cause memory leak.

201512290192

- Symptom: CVE-2015-3196
- Condition: Fixed vulnerability where a race condition can occur when specific PSK identity hints are received.

201512290192

- Symptom: CVE-2015-1794
- Condition: Fixed vulnerability if a client receives a ServerKeyExchange for an anonymous Diffie-Hellman (DH) ciphersuite which can cause possible Denial of Service (DoS) attack.

Resolved problems in R3112

201602040025

- Symptom: After the **lldp notification med-topology-change enable** command is executed on a PoE-capable switch, the LLDP process exits unexpectedly and the IP phones connected to the PIs of the switch cannot operate correctly.
- Condition: This symptom might occur if the command is executed on a PoE-capable switch and IP phones are connected to the PIs of the switch.

201601110412

- Symptom: The CPU usage of an IRF fabric is high if LLDP is enabled on a large number of up interfaces.
- Condition: This symptom might occur if LLDP is enabled for a large number of up interfaces on an IRF fabric.

201602170470

- Symptom: The add or remove DNS server IP operation fails on the **Network** > **DNS** page of the Web interface.
- Condition: This symptom might occur if a DNS server IP address is added or removed on the **Network** > **DNS** page of the Web interface.

201601270478

- Symptom: The **Resources** > **PKI** page of the Web interface stays in the loading status.
- Condition: This symptom might occur if the **Resources** > **PKI** page of the Web interface is accessed.

201603100197

- Symptom: On an inactivity aging-enabled interface, sticky MAC addresses age out before the secure MAC aging timer set by using the **port-security timer autolearn aging** command expires.
- Condition: This symptom might occur if the following operations are performed on an interface:
  - Enable port security and inactivity aging.
  - Use the **port-security timer autolearn aging** command to set the secure MAC aging timer.

201601280398

- Symptom: When the Firefox browser is used to access the Web interface, the dropdown lists on some pages are unavailable.
- Condition: This symptom might occur if the Firefox browser is used to perform one of the following operations:

- Add IPv4 static routes on the **Network** > **Static Routing** page.
- Create a rate limit for an interface on the **QoS** > **Rate Limit** page.
- Configure IRF port bindings on the **Device** > **IRF** page.

Resolved problems in R3111P07

201512130013

- Symptom: An interface in a VLAN mapped to an MSTI fails to be assigned to the MSTI.
- Condition: This symptom might occur if the link type of the interface is changed between trunk and access repeatedly.

201601130674

- Symptom: After a user exits the console login page, the user cannot log in to the switch again through the console port.
- Condition: This symptom occurs if the **restore factory-default** command is executed to restore factory default configuration.

201601180281

- Symptom: A Web page is incorrectly displayed. To display the correct page, you must refresh the page.
- Condition: This symptom occurs if you access the **Device**, **Network**, or **QoS** page first through Web and then access other pages.

201512230197

- Symptom: The PoE status is incorrectly displayed for an interface.
- Condition: This symptom occurs if you access the PoE configuration page of a PoE switch through Web.

201511160443

- Symptom: During 802.1X authentication that uses the EAP method, the RADIUS packets exchanged in one user authentication process might be sent to different servers.
- Condition: This symptom occurs if RADIUS server load sharing is enabled on the switch.

201507310169

- Symptom: The subordinate IRF member switch might reboot unexpectedly.
- Condition: This symptom might occur if patches are repeatedly installed and removed in an IRF fabric.

Resolved problems in R3111P03

201511300121

- Symptom: The switch acting as an NTP client cannot be synchronized to an NTP server.
- Condition: This symptom occurs if the NTP server is a Cisco device.

201510300354

- Symptom: A user goes offline immediately after the user comes online through 802.1X authentication.
- Condition: This symptom occurs if the following conditions exist:
  - Another user comes online through MAC authentication before the 802.1X user.

- The 802.1X user is assigned the same VLAN as the MAC-authenticated user.

201512090334

- Symptom: The operation of backing up the configuration file fails.
- Condition: This symptom occurs if the following conditions exist:
  - The MIB node hh3cCfgOperateServerAddress is configured to specify the file backup server.
  - The IP address of the file backup server is in the range of x.x.x.224 to x.x.x.255.

201511180177

- Symptom: A port cannot exit the guest VLAN.
- Condition: This symptom occurs if the following conditions exist:
  - The switch is enabled with 802.1X.
  - The port joins the 802.1X guest VLAN.
  - The MAC address of the MAC-VLAN entry has been learned by another port.

201511190408

- Symptom: CVE-2015-7871
- Condition: Cause ntpd to accept time from unauthenticated peers.

201511190408

- Symptom: CVE-2015-7704
- Condition: An ntpd client forged by a DDoS attacker located anywhere on the Internet, that can exploit NTP's to disable NTP at a victim client or it may also trigger a firewall block for packets from the target machine.

201511190408

- Symptom: CVE-2015-7705
- Condition: The DDoS attacker can send a device a high volume of ntpd queries that are spoofed to look like they come from the client. The servers then start rate-limiting the client.

201511190408

- Symptom: CVE-2015-7855
- Condition: Ntpd mode 6 or mode 7 packet containing an unusually long data value could possibly use cause NTP to crash, resulting in a denial of service.

201501160412

- Symptom: The switch cannot send trap messages if it is rebooted after SNMP is configured. The switch can send trap messages correctly if it is rebooted again.
- Condition: This symptom might occur if the following operations have been performed:
  - Configure SNMP.
  - Save the configuration and reboot the switch.
  - Enter the CLI and do not execute any commands.

201511230171

- Symptom: The CPU occupied by the aclmgrd process is not released. As a result, the CPU usage of the switch is high.
- Condition: This symptom occurs if master/subordinate switchover occurs in an IRF fabric.

Resolved problems in R3111P02

201512200032

- Symptom: On an IRF fabric enabled with 802.1X or MAC authentication, the CPU usage is high on the member switches that do not reboot after an active/standby MPU switchover occurs.
- Condition: This symptom might occur if 802.1X or MAC authentication is configured on the IRF fabric, and an active/standby MPU switchover occurs.

Resolved problems in R3111P01

201512040456

- Symptom: A subordinate switch in an IRF fabric reboots repeatedly.
- Condition: This symptom occurs if the .mdb file is deleted and the IRF fabric is power cycled.

201505150471

- Symptom: A subordinate switch in an IRF fabric cannot discover neighbors because it cannot forward LLDP frames.
- Condition: This symptom occurs if the **l2protocol lldp tunnel dot1q** command is configured on an interface on the subordinate switch.

201511190389

- Symptom: The CPU usage of an IRF fabric is high.
- Condition: This symptom occurs if the following conditions exist:
  - A VLAN interface on the IRF fabric is configured with an IP address.
  - A member switch in the IRF fabric is configured as a DHCP server.

Resolved problems in R3110

201511190084

- Symptom: The switch treats an **Apply-Actions** instruction in an OpenFlow flow entry as a Write**-Actions** instruction.
- Condition: This symptom occurs if the controller deploys a flow entry with an **Apply-Actions** instruction.

201510280475

- Symptom: A user goes offline immediately after the user comes online through 802.1X authentication.
- Condition: This symptom occurs if the switch uses a RADIUS scheme and local accounting for 802.1X authentication.

201511180069

- Symptom: The first 24 ports on a 52-port switch cannot communicate with the last 24 ports on the switch.
- Condition: This symptom might occur if the switch is rebooted repeatedly.

201508170320

- Symptom: The value of the entPhysicalVendorType node for a transceiver module cannot be obtained through a MIB tool.

- Condition: This symptom occurs if the following operations have been performed:
  - Use the **combo enable fiber** command on a combo interface to activate its fiber combo port.
  - Install the transceiver module into the fiber combo port.

201511170067

- Symptom: OpenFlow flow entries fail to be deployed.
- Condition: This symptom occurs if the controller deploys flow entries without actions to a flow table other than the first flow table of the multiple flow tables.

Resolved problems in R3109P16

201507160220

- Symptom: CVE-2014-8176
- Condition: If a DTLS peer receives application data between the ChangeCipherSpec and Finished messages. May result in a segmentation fault or potentially, memory corruption.

201507160220

- Symptom:CVE-2015-1788
- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

201507160220

- Symptom: CVE-2015-1789
- Condition: X509_cmp_time does not properly check the length of the ASN1_TIME string and/or accepts an arbitrary number of fractional seconds in the time string. An attacker can use this to craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS on applications that verify certificates or CRLs.

201507160220

- Symptom: CVE-2015-1790
- Condition: The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201507160220

- Symptom: CVE-2015-1791
- Condition: If a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket then a race condition can occur potentially leading to a double free of the ticket data.

201507160220

- Symptom: CVE-2015-1792
- Condition: When verifying a signedData message the CMS code can enter an infinite loop. This can be used to perform denial of service against any system which verifies signedData messages using the CMS code.

Resolved problems in R3109P14

201504130201

- Symptom: After successful 802.1X authentication, a port sets the tagging status to untagged for packets of a voice VLAN. As a result, IP phones receive untagged packets.
- Condition: This symptom might occur if the following conditions exist:
  - 802.1X authentication and voice VLAN are configured on the port.
  - The device-traffic-class=voice attribute is configured on the authentication server.

201509020039

- Symptom: User authentication fails.
- Condition: This symptom occurs if the switch uses an ACS 5.6 server to perform AAA authentication.

201509160335

- Symptom: User authentication fails.
- Conditions: This symptom occurs if the PEAP authentication method is used to perform 802.1X authentication.

201509100463

- Symptom: The OpenFlow process restarts when the switch is receiving flow entries from the controller.
- Condition: This symptom might occur if the switch is receiving flow entries from the controller.

201509110280

- Symptom: The switch performs 802.1X reauthentication when it receives an EAPOL-Start message from a Windows client. After several reauthentication failures, the Windows client is put in silent state, and its NIC becomes unavailable.
- Condition: This symptom might occur if the following conditions exist:
  - 802.1X authentication and voice VLAN are configured on the switch.
  - The authentication server is unreachable, and the Windows client is in the 802.1X critical VLAN.

201509260060

- Symptom: The Web interface is slow in refreshing webpages or does not respond when PoE is configured for an IRF fabric.
- Condition: This symptom might occur if the Web interface is used to configure PoE for an IRF fabric.

201510130396

- Symptom: Some services might operate incorrectly or the switch might reboot unexpectedly.
- Condition: This symptom occurs when a MIB management tool is used to obtain the power supply information of the switch.

Resolved problems in R3109P09

201509010289

- Symptom: The switch logs out a MAC-authenticated user that sends packets to the switch before the offline detect timer expires.

- Condition: This symptom might occur if MAC authentication is configured.

201508080233

- Symptom: The switch cannot start up.
- Condition: This symptom occurs if the switch's flash memory is corrupted.

201508310155

- Symptom: An interface advertises an Auto-negotiation TLV with an incorrect value and fails to negotiate with the peer interface.
- Condition: This symptom occurs when LLDP is enabled globally and on the interface.

201508120317

- Symptom: The **poe max power** configuration is automatically generated for an interface after the connected IP phone sends an LLDP frame to request power.
- Condition: This symptom might occur if the connected IP phone sends an LLDP frame to request power from the interface.

201509010156

Symptom: The following switch models support the power design daughter card:

- HP 5130-24G-PoE+-4SFP+ (370W) EI Switch JG936A.
- HP 5130-48G-PoE+-4SFP+ (370W) EI Switch JG937A.
- HP 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A.
- HP 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A.

Condition: None.

201506180249

- Symptom: CVE-2015-3143
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request.

201506180249

- Symptom: CVE-2015-3148
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

Resolved problems in R3109P07

201506100324

- Symptom: Software upgrade fails for an IRF fabric from the Web interface.
- Conditions: This symptom might occur when you upgrade software for the IRF fabric from the Web interface.

201503050138

- Symptom: The flash memory of an IRF subordinate device is not available after the device reboots to rejoin the IRF fabric.
- Conditions: This symptom might occur if you have saved running configuration only for this subordinate device in the IRF fabric before you reboot the device.

201504090194

- Symptoms: CVE-2015-0209

- Condition: A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources.

201504090194

- Symptoms: CVE-2015-0286
- Condition: DoS vulnerability in certificate verification operation. Any application which performs certificate verification is vulnerable including OpenSSL clients and servers which enable client authentication.

201504090194

- Symptoms: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

201504090194

- Symptoms:CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.

201504090194

- Symptoms: CVE-2015-0289
- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201505150249

- Symptom: TCP processing errors occur during an NQA operation. The operation fails, and services are interrupted on the switch.
- Condition: This symptom might occur if an NQA operation is performed on the switch.

201505150245

- Symptom: The switch cannot correctly send ARP packets to the controller.
- Condition: This symptom might occur if a .mdb binary configuration file is used to restore OpenFlow configuration.

201504200256

- Symptom: The switch cannot provide DHCP services correctly as a DHCP server.
- Condition: This symptom might occur if the following conditions exist:
  - A DHCP client has obtained an IP address from the DHCP server, and its address lease expires.
  - The client is configured as a BOOTP client.

201505240024

- Symptom: Some PoE registers restore the default values after the PoE firmware is online updated.
- Condition: This symptom might occur if a PoE firmware online update is performed.

201506170069

- Symptom: An 802.1X client is forced to log off soon after it logs in.
- Condition: This symptom occurs if the 802.1X authentication server assigns security policies such as ACL and user profile to the client after the client passes the 802.1X authentication.

Resolved problems in R3109P05

201505150457

- Symptom: A PoE switch cannot supply power over PoE to IP phones of some vendors.
- Condition: This symptom occurs when you connect the IP phones to the switch and supply power over PoE.

201506130010

- Symptom: A port is brought up and can forward packets when the MDIX mode negotiation fails.
- Condition: This symptom occurs if the following operations have been performed:
  - Use a straight-through cable to connect the port and its peer port.
  - Configure the same MDI (or MDIX) mode at both ends of the cable.

201504020079

- Symptom: The Web interface is stuck at the **Please wait…** window when you upgrade system software in the Web interface.
- Condition: This symptom occurs after you select the upgrade file and click **Apply** in the Web interface.

201502110444

- Symptom: The switch reconnects to the SDN controller immediately after an unexpected disconnection from the controller.
- Condition: This symptom might occur if an active/standby MPU switchover occurs when the controller is issuing a large number of flow table entries to the switch.

201506100226

- Symptom: The port connected to an IP phone is removed from the voice VLAN after both the LLDP aging timer and the voice VLAN aging timer expire.
- Condition: This symptom might occur if the switch establishes a neighbor relationship with the IP phone and advertises voice VLAN information to the IP phone through LLDP.

201504210120

- Symptom: The PSE status setting of an IRF fabric is missing after a subordinate switch is rebooted.
- Condition: This symptom might occur if the following conditions exist:
  - The IRF fabric contains multiple members.
  - The **poe enable pse** command is configured on the IRF fabric.
  - The subordinate switch is a PoE switch.

201505110287

- Symptom: A user passes MAC authentication, but the authentication server fails to assign the authorization VLAN to the user.
- Condition: This symptom occurs if the VLAN attribute issued by the authentication server in the Access-Accept packet ends with **\0x00**.

201504150187

- Symptom: CVE-2015-1799
- Condition: Authentication doesn’t protect symmetric associations against DoS attacks.

201505270138

- Symptom: The switch cannot use IP subnet-based VLANs to match and forward untagged packets.
- Condition: This symptom might occur if IP subnet-based VLANs are configured on the switch.

201412120103

- Symptom: After a reboot, the IDs of some members in an IRF fabric are changed to the default number 1. The affected members cannot rejoin the IRF fabric.
- Condition: This symptom might occur if operations are frequently performed on the NOR flash memory, for example, save the configuration file frequently.

201505110140

- Symptom: The switch reboots unexpectedly or cannot provide services correctly when a MAC address move occurs.
- Condition: This symptom might occur if one of the following conditions exists on the switch:
  - 100 or more ARP entries in a VLAN have the same MAC address, and the MAC address moves between ports.
  - The MAC address of an ARP entry moves between ports five times per second or more frequently.

Resolved problems in R3109P04

201505240023

- Symptom: A PoE switch fails to supply power over PoE to all PDs after the switch is power cycled.
- Condition: This symptom might occur after the switch is power cycled.

201510130155

- Symptom: The switch fails to obtain an IP address across VLANs.
- Condition: This symptom might occur if the following conditions exist:
  - A Layer 3 firewall is not deployed between the switch and the DHCP server.
  - DHCP relay is enabled on the Layer 3 firewall, and DHCP snooping is enabled on the switch.

Resolved problems in R3109P03

201503310150

- Symptom: A PC cannot obtain an IP address from the DHCP server.
- Condition: This symptom occurs if the following conditions exist:
  - DHCP snooping is enabled by using the **dhcp snooping enable** command on the switch.
  - The private VLAN feature is configured on the switch.
  - An interface in a primary VLAN is connected to the DHCP server.
  - An interface in an associated secondary VLAN is connected to the PC.

201504080340

- Symptom: A RADIUS server fails to identify Access-Request packets from the switch, and users fail the authentication.

- Condition: This symptom occurs if Access-Request packets include invalid attribute values, for example, attribute values that end with **\0**.

Resolved problems in R3109P01

201501290379

- Symptom: 802.1X users fail to log in.
- Condition: This symptom occurs if the authorization VLANs assigned by the authentication server use a format incompatible with the switch.

201412180459

- Symptom: Traffic is not forwarded based on an OpenFlow group entry as expected.
- Condition: This symptom occurs if the following operations have been performed:
  - Configure a group entry.
  - Deploy a flow entry and configure the flow entry to use the group entry for forwarding.
  - Modify the output port of the group entry.

201412150089

- Symptom: Portal users log out unexpectedly.
- Condition: This symptom occurs if the following conditions exist:
  - DHCP and portal roaming are enabled.
  - The portal users roam between APs by using mobile devices.

201503020204

- Symptom: A PoE switch cannot supply power correctly.
- Condition: This symptom occurs if the PoE module receives incorrect instructions.

201412190083

- Symptom: The **voice-vlan qos** command does not take effect on an interface.
- Condition: This symptom occurs if CDP-compatible LLDP is configured to advertise voice VLAN information on the interface.

201501210272

- Symptom: CVE-2014-3569
- Condition: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling.

201501210272

- Symptom: CVE-2014-3571
- Condition: A carefully crafted DTLS message can cause a segmentation fault in OpenSSL due to a NULL pointer dereference. This could lead to a Denial Of Service attack.

201501210272

- Symptom: CVE-2015-0206
- Condition: A memory leak can occur in the dtls1_buffer_record function under certain conditions. In particular this could occur if an attacker sent repeated DTLS records with the

same sequence number but for the next epoch. The memory leak could be exploited by an attacker in a Denial of Service attack through memory exhaustion.

201501210272

- Symptom: CVE-2015-0205
- Condition: An OpenSSL server will accept a DH certificate for client authentication without the certificate verify message. This effectively allows a client to authenticate without the use of a private key. This only affects servers which trust a client certificate authority which issues certificates containing DH keys.

201501210272

- Symptom: CVE-2014-3570
- Condition: Bignum squaring (BN_sqr) may produce incorrect results on some platforms, including x86_64. This bug occurs at random with a very low probability, and is not known to be exploitable in any way.

201501210272

- Symptom: CVE-2015-0204
- Condition: An OpenSSL client will accept the use of an RSA temporary key in a non-export RSA key exchange ciphersuite. A server could present a weak temporary key and downgrade the security of the session.

201501210272

- Symptom: CVE-2014-3572
- Condition: An OpenSSL client will accept a handshake using an ephemeral ECDH ciphersuite using an ECDSA certificate if the server key exchange message is omitted. This effectively removes forward secrecy from the ciphersuite.

201501210272

- Symptom: CVE-2014-8275
- Condition: By modifying the contents of the signature algorithm or the encoding of the signature, it is possible to change the certificate's fingerprint. Only custom applications that rely on the uniqueness of the fingerprint may be affected.

Resolved problems in R3108P03

201412150184

- Symptom: The MAC address entry for a user successfully passing MAC authentication is aged before the offline detect timer expires.
- Condition: This symptom occurs when MAC authentication is enabled and the **mac-authentication timer offline-detect** command is used set the offline detect timer for MAC authentication.

201501140409

- Symptom: A user passing MAC authentication must wait 60 seconds before triggering new MAC authentication.
- Condition: This symptom occurs when the following conditions exist:
  - MAC authentication is enabled on an interface.
  - A user that accesses the interface passes MAC authentication.
  - The **shutdown** and then **undo shutdown** commands are executed on the interface.

201412150398

- Symptom: After the **shutdown** command is executed in an interface through which a user fails the 802.1X authentication, the interface is still in the 802.1X Auth-Fail VLAN configured for the interface.
- Condition: This symptom occurs when the following conditions exist:
  - The **dot1x quiet-period** command is used in system view to enable the quiet timer.
  - 802.1X is enabled on the interface.
  - An 802.1X Auth-Fail VLAN is configured on the interface.

201412040514

- Symptom: The switch first replies with a barrier reply and then prompts an error.
- Condition: This symptom occurs when OpenFlow continues to deploy flow entries and sends barrier request messages after the deployed flow entries reach the specifications.

201412310374

- Symptom: CVE-2014-9295.
- Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet.

201410230226

- Symptom: SSL 3.0 Fallback protection.
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

201410230226

- Symptom: CVE-2014-3567
- Condition: When an OpenSSL SSL/TLS/DTLS server receives a session ticket the integrity of that ticket is first verified. In the event of a session ticket integrity check failing, OpenSSL will fail to free memory causing a memory leak. By sending a large number of invalid session tickets an attacker could exploit this issue in a Denial of Service attack.

201501150467

- Symptom: PoE cannot supply power correctly.
- Condition: This symptom can be seen when the PoE chip becomes abnormal because of PoE communication errors.

201501070257

- Symptom: The switch cannot communicate with a Cisco IP phone.
- Condition: This symptom can be seen when the following conditions exist:
  - The switch is directly connected to the Cisco IP phone.
  - CDP-compatible LLDP is enabled on the switch.
  - The sent LLDP protocol packets and CDP protocol packets carry voice VLAN TLVs.

201407310086

- Symptom: The function of configuring the voice VLAN information that LLDP/CDP advertises does not take effect.

- Condition: This symptom can be seen when the **lldp tlv-enable med-tlv network-policy** *vlan-id* command is configured on an interface to specify the voice VLAN information that LLDP/CDP will advertise to IP phones.

Resolved problems in R3108P01

201410140175

- Symptom: The system displays configuration errors though the configuration has been issued to an interface.
- Condition: This symptom can be seen when you log in to the switch through the Web interface and shut down an IRF physical interface.

201410210187

- Symptom: When a user performs MAC authentication, the system does not transmit information about the MAC authentication-enabled interface to the authentication server. As a result, the user fails to pass the authentication.
- Condition: This symptom can be seen after you log in to the switch through the Web interface and enable MAC authentication on the interface.

201410200402

- Symptom: The number of 802.1X online users collected in the Web interface is different from the actual number of 802.1X online users.
- Condition: This symptom can be seen when 2000 users pass 802.1X authentication and come online.

201408290076

- Symptom: PoE cannot be successfully enabled on a port.
- Condition: This symptom can be seen when you log in to the switch through the Web interface and enable PoE on the port.

201410200322

- Symptom: The maximum power of a PSE cannot be restored to the original value.
- Condition: This symptom can be seen when the following procedure is performed:
  - Log in to the switch through the Web interface.
  - Input an incorrect value for the maximum PSE power.
  - Clic**k Cancel**.

201410100091

- Symptom: A black screen appears on the Web login page for the switch.
- Condition: This symptom can be seen when you log in to the switch through the Web interface and test the cable connections for Ethernet interfaces of the switch multiple times.

201312030126

- Symptom: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.
- Condition: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.

201410210004

- Symptom: Device will tear down TCP connection in established state when receives wrong TCP packet.

- Condition: Only for those TCP connections in established state. When they receive TCP SYN packet which is carrying a sequence number falling into the connection receiving window, a RST packet will be sent and the connection will be dropped immediately.

201406190088

- Symptom: CVE-2014-0224.
- Condition: This symptom can be seen when Open SSL Server is used.

201408220480

- Symptom: CVE-2014-3508
- Condition: A flaw in OBJ_obj2txt may cause pretty printing functions such as X509_name_oneline, X509_name_print_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

201406270104

- Symptom: The MAC address entries of an STP edge port are deleted if the network topology changes.
- Condition: This symptom might occur if a port is configured as an STP edge port, and network topology changes occur.

Resolved problems in R3106P01

None

Resolved problems in R3106

First release

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect:

- Technical support registration number (if applicable).
- Product name, model or version, and serial number.
- Operating system name and version.
- Firmware version.
- Error messages.
- Product-specific reports and logs.
- Add-on products or components.
- Third-party products or components.

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website at http://www.hpe.com/support/hpesc.

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see HPE FlexNetwork technology acronyms.

Related documents

The following documents provide related information:

- HPE 5130 EI Switch Series Installation Guide
- HPE PSR150-A & PSR150-D Power Supplies User Guide
- HPE 5130 EI Switch Series Configuration Guides-Release 32xx
- HPE 5130 EI Switch Series Command References-Release 32xx

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Appendix A Feature list

Hardware features

Refer to *HPE 5130 EI Switch Series Installation Guide*

Software features

Table 4 Software features of the 5130 EI series

Feature	HPE 5130-24G-4SFP+ EI Switch / HPE 5130-24G-2SFP+-2XGT EI Switch/ HPE 5130-24G-4SFP+ EI Brazil Switch	HPE 5130-48G-4SFP+ EI Switch / HPE 5130-48G-2SFP+-2XGT EI Switch/ HPE 5130-48G-4SFP+ EI Brazil Switch	HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch / HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch/ HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch	HPE 5130-24G-SFP-4SFP+ EI Switch	HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch / HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch/ HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch
Forwarding mode	Store-forward				
IRF	• Ring topology • Daisy chain topology • LACP MAD • ARP MAD • ND MAD • BFD MAD • IRF comprised of different models				
Link aggregation	• Aggregation of 10-GE ports • Aggregation of GE ports • Static link aggregation • Dynamic link aggregation • Inter-device aggregation • A maximum of 14 aggregation groups on a device • A maximum of 128 inter-device aggregation groups • A maximum of 8 ports for each aggregation group				
Flow control	• IEEE 802.3x flow control • Back pressure				
Jumbo Frame	• Supports maximum frame size of 9000				
MAC address table	• 16K MAC addresses • 1K static MAC addresses				

	• Blackhole MAC addresses • MAC address learning limit on a port
VLAN	• Port-based VLANs (4094 VLANs) • QinQ and selective QinQ
VLAN mapping	• One-to-one VLAN mapping • Many-to-one VLAN mapping • Two-to-two VLAN mapping
ARP	• 1K entries • 512 static entries • Gratuitous ARP • Common proxy ARP and local proxy ARP • ARP source suppression • ARP black hole • ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings) • Multiport ARP
ND	• 512 entries • 256 static entries
VLAN virtual interface	32
DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server • DHCPv6 server • DHCPv6 relay agent • DHCPv6 snooping
UDP helper	• UDP helper
DNS	• Static DNS • Dynamic DNS • IPv4 and IPv6 DNS
IPv4 unicast route	• 512 static routes • RIP • Routing policies • Policy-based routing
IPv6 unicast route	• 256 static routes • RIPng • Routing policies • Policy-based routing
BFD	• Static route • MAD
Multicast	• IGMP snooping • MLD snooping • IPv4 and IPv6 multicast VLAN • IPv4 and IPv6 PIM snooping
Broadcast/multicast/unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Bps-based storm control

MSTP	• STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard • 128 PVST instances
QoS/ACL	• Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4) • Eight output queues for each port • SP/WRR/SP+WRR queue scheduling algorithms • Port-based rate limiting • Flow-based redirection • Time range
Mirroring	• Stream mirroring • Port mirroring • Multiple mirror observing port
Remote mirroring	• Port remote mirroring (RSPAN)
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • 802.1X • Port security • MAC-address-based authentication • IP Source Guard • HTTPS • PKI • EAD
802.1X	• Up to 2,048 users • Port-based and MAC address-based authentication • Trunk port authentication • Dynamic 802.1X-based QoS/ACL/VLAN assignment
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • IMC NMS • System log • Hierarchical alarms • NTP • Power supply alarm function • Fan and temperature alarms
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track

	• Remote maintenance through Telnet • 802.1ag • 802.3ah • DLDP

Appendix B Fixed security vulnerabilities

Fixed security vulnerabilities in R3507P09

CVE-2015-2808

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah"

CVE-2022-0778

A flaw was found in OpenSSL. It is possible to trigger an infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens before verification of the certificate signature, any process that parses an externally supplied certificate may be subject to a denial of service attack.

CVE-2021-4160

There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

Appendix C Upgrading software

This chapter describes types of software used on the switch and how to upgrade software while the switch is operating normally or when the switch cannot correctly start up.

System software file types

Software required for starting up the switch includes:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the switch cannot correctly start up.
- **Software images**—Includes boot images and system images.
  - **Boot image**—A .bin file that contains the operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
  - **System image**—A .bin file that contains the minimum modules required for device operation and some basic features, including device management, interface management, configuration management, and routing management.

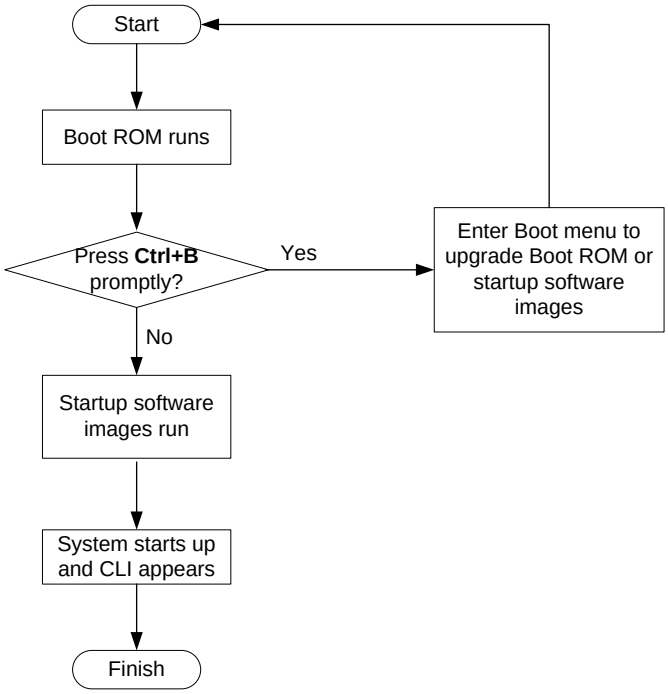
  The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images in the file and sets them as startup software images. Typically, the Boot ROM and software images for this switch series are released in an .ipe file named **main.ipe**.

System startup process

Upon power-on, the Boot ROM image runs to initialize hardware and then the software images run to start up the entire system, as shown in Figure 1.

Figure 1 System startup process



Upgrade methods

You can upgrade system software by using one of the following methods:

Upgrading method	Software types	Remarks
Upgrading from the CLI	• Boot ROM image • Software images	• You must reboot the switch to complete the upgrade. • This method can interrupt ongoing network services.
Upgrading from the Boot menu	• Boot ROM image • Software images	Use this method when the switch cannot correctly start up. **△ CAUTION:** Upgrading an IRF fabric from the CLI instead of the Boot menu. The Boot menu method increases the service downtime, because it requires that you upgrade the member switches one by one.

The output in this document is for illustration only and might vary with software releases. This document uses boot.bin and system.bin to represent boot and system image names. The actual software image name format is *chassis-model_Comware-version_image-type_release*, for example, 5130EI-CMW710-BOOT-R3115P01.bin and 5130EI-CMW710-SYSTEM-R3115P01.bin.

Upgrading from the CLI

This section uses a two-member IRF fabric as an example to describe how to upgrade software from the CLI. If you have more than two subordinate switches, repeat the steps for the subordinate switch to upgrade their software. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch. For more information about setting up and configuring an IRF fabric, see the installation guide and IRF configuration guide for the HPE 5130 EI switch series.

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

1. Log in to the IRF fabric through Telnet or the console port. (Details not shown.)
2. Identify the number of IRF members, each member switch's role, and IRF member ID.

```
<Sysname> display irf
MemberID   Role   Priority  CPU-Mac         Description
 *+1       Master  5         0023-8927-afdc  ---
   2       Standby 1         0023-8927-af43  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-8927-afdb
 Auto upgrade               : no
 Mac persistent             : 6 min
 Domain ID                  : 0
```

3. Verify that each IRF member switch has sufficient storage space for the upgrade images.

IMPORTANT:

Each IRF member switch must have free storage space that is at least two times the size of the upgrade image file.

Identify the free flash space of the master switch.

```
<Sysname> dir
Directory of flash:
     0      -rw-       41424  Aug 23 2013 02:23:44     startup.mdb
     1      -rw-        3792  Aug 23 2013 02:23:44     startup.cfg
     2      -rw-    53555200  Aug 23 2013 09:53:48     system.bin
     3      drw-           -  Aug 23 2013 00:00:07     seclog
     4      drw-           -  Aug 23 2013 00:00:07     diagfile
     5      drw-           -  Aug 23 2013 00:00:07     logfile
     6      -rw-     9959424  Aug 23 2013 09:53:48     boot.bin
     7      -rw-     9012224  Aug 23 2013 09:53:48     backup.bin

524288 KB total (453416 KB free)
```

Identify the free flash space of each subordinate switch, for example, switch 2.

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:/
     0      -rw-       41424  Jan 01 2011 02:23:44     startup.mdb
```

```
1       -rw-         3792  Jan 01 2011 02:23:44     startup.cfg
2       -rw-     93871104  Aug 23 2013 16:00:08     system.bin
3       drw-            -  Jan 01 2011 00:00:07     seclog
4       drw-            -  Jan 01 2011 00:00:07     diagfile
5       drw-            -  Jan 02 2011 00:00:07     logfile
6       -rw-     13611008  Aug 23 2013 15:59:00     boot.bin
7       -rw-      9012224  Nov 25 2011 09:53:48     backup.bin

524288 KB total (453416 KB free)
```

4. Compare the free flash space of each member switch with the size of the software file to load. If the space is sufficient, start the upgrade process. If not, go to the next step.
5. Delete unused files in the flash memory to free space:

CAUTION:

- To avoid data loss, do not delete the current configuration file. For information about the current configuration file, use the **display startup** command.
- The **delete /unreserved** *file-url* command deletes a file permanently and the action cannot be undone.
- The **delete** *file-url* command moves a file to the recycle bin and the file still occupies storage space. To free the storage space, first execute the **undelete** command to restore the file, and then execute the **delete /unreserved** *file-url* command.

Delete unused files from the flash memory of the master switch.

```
<Sysname> delete /unreserved flash:/backup.bin
The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/backup.bin...Done.
# Delete unused files from the flash memory of the subordinate switch.
<Sysname> delete /unreserved slot2#flash:/backup.bin
The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file slot2#flash:/backup.bin...Done.
```

Downloading software images to the master switch

Before you start upgrading software images packages, make sure you have downloaded the upgrading software files to the root directory in flash memory. This section describes downloading an .ipe software file as an example.

The following are ways to download, upload, or copy files to the master switch:

- FTP download from a server
- FTP upload from a client
- TFTP download from a server

Prerequisites

If FTP or TFTP is used, the IRF fabric and the PC working as the FTP/TFTP server or FTP client can reach each other.

Prepare the FTP server or TFTP server program yourself for the PC. The switch series does not come with these software programs.

FTP download from a server

You can use the switch as an FTP client to download files from an FTP server.

To download a file from an FTP server, for example, the server at 10.10.110.1:

1. Run an FTP server program on the server, configure an FTP username and password, specify the working directory and copy the file, for example, **newest.ipe**, to the directory.
2. Execute the **ftp** command in user view on the IRF fabric to access the FTP server.

```
<Sysname> ftp 10.10.110.1
Trying 10.10.110.1...
Press CTRL+C to abort
Connected to 10.10.110.1(10.10.110.1).
220 FTP service ready.
User (10.10.110.1:(none)):username
331 Password required for username.
Password:
230 User logged in.
```

3. Enable the binary transfer mode.

```
ftp> binary
  200 Type set to I.
```

4. Execute the **get** command in FTP client view to download the file from the FTP server.

```
ftp> get newest.ipe
  227 Entering Passive Mode (10,10,110,1,17,97).
  125 BINARY mode data connection already open, transfer starting for /newest.ipe
  226 Transfer complete.
  32133120 bytes received in 35 seconds (896. 0 kbyte/s)
ftp> bye
221 Server closing.
```

FTP upload from a client

You can use the IRF fabric as an FTP server and upload files from a client to the IRF fabric.

To FTP upload a file from a client:

On the IRF fabric:

1. Enable FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

2. Configure a local FTP user account:

   # Create the user account.

```
[Sysname] local-user abc
```

   # Set its password and specify the FTP service.

```
[Sysname-luser-manage-abc] password simple pwd
[Sysname-luser-manage-abc] service-type ftp
```

   # Assign the **network-admin** user role to the user account for uploading file to the working directory of the server.

```
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
[Sysname-luser-manage-abc] quit
[Sysname] quit
```

On the PC:

3. Log in to the IRF fabric (the FTP server) in FTP mode.

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
```

```
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

4. Enable the binary file transfer mode.

```
ftp> binary
200 TYPE is now 8-bit binary.
```

5. Upload the file (for example, **newest.ipe**) to the root directory of the flash memory on the master switch.

```
ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 32133120 bytes sent in 64.58 secs (497.60 Kbytes/sec).
```

TFTP download from a server

To download a file from a TFTP server, for example, the server at 10.10.110.1:

1. Run a TFTP server program on the server, specify the working directory, and copy the file, for example, newest.ipe, to the directory.
2. On the IRF fabric, execute the tftp command in user view to download the file to the root directory of the flash memory on the master switch.

```
<Sysname> tftp 10.10.110.1 get newest.ipe
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 30.6M    0 30.6M    0     0   143k      0 --:--:--  0:03:38 --:--:--  142k
```

Upgrading the software images

To upgrade the software images:

1. Specify the upgrade image file (**newest.ipe** in this example) used at the next startup for the master switch, and assign the M attribute to the boot and system images in the file.

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
Verifying image file.........Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin...................Done.
Decompressing file system.bin to flash:/system.bin...............Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 1.
```

2. Specify the upgrade image file as the main startup image file for each subordinate switch. This example uses IRF member 2. (The subordinate switches will automatically copy the file to the root directory of their flash memories.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
Verifying image file.........Done.
```

```
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin.....................Done.
Decompressing file system.bin to flash:/system.bin................Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 2.
```

3. Enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
[Sysname] quit
```

This function checks the software versions of member switches for inconsistency with the master switch. If a subordinate switch is using a different software version than the master, the function propagates the current software images of the master to the subordinate as main startup images. The function prevents software version inconsistency from causing the IRF setup failure.

4. Save the current configuration in any view to prevent data loss.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.................
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
This command will reboot the device. Continue? [Y/N]:y
 Now rebooting, please wait...
```

The system automatically loads the .bin boot and system images in the .ipe file and sets them as the startup software images.

6. Execute the **display version** command in any view to verify that the current main software images have been updated (details not shown).

NOTE:

The system automatically checks the compatibility of the Boot ROM image and the boot and system images during the reboot. If you are prompted that the Boot ROM image in the upgrade image file is different than the current Boot ROM image, upgrade both the basic and extended sections of the Boot ROM image for compatibility. If you choose to not upgrade the Boot ROM image, the system will ask for an upgrade at the next reboot performed by powering on the switch or rebooting from the CLI (promptly or as scheduled). If you fail to make any choice in the required time, the system upgrades the entire Boot ROM image.

Upgrading from the Boot menu

In this approach, you must access the Boot menu of each member switch to upgrade their software one by one. If you are upgrading software images for an IRF fabric, using the CLI is a better choice.

TIP:
Upgrading through the Ethernet port is faster than through the console port.

Prerequisites

Make sure the prerequisites are met before you start upgrading software from the Boot menu.

Setting up the upgrade environment

1. Use a console cable to connect the console terminal (for example, a PC) to the console port on the switch.
2. Connect the Ethernet port on the switch to the file server.

NOTE:
The file server and the configuration terminal can be co-located.

3. Run a terminal emulator program on the console terminal and set the following terminal settings:
   - **Bits per second**—9,600
   - **Data bits**—8
   - **Parity**—None

Stop bits—1

   - **Flow control**—None
   - **Emulation**—VT100

Preparing for the TFTP or FTP transfer

To use TFTP or FTP:

- Run a TFTP or FTP server program on the file server or the console terminal.
- Copy the upgrade file to the file server.
- Correctly set the working directory on the TFTP or FTP server.
- Make sure the file server and the switch can reach each other.

Verifying that sufficient storage space is available

IMPORTANT:
For the switch to start up correctly, do not delete the main startup software images when you free storage space before upgrading Boot ROM. On the Boot menu, the main startup software images are marked with an asterisk (*).

When you upgrade software, make sure each member switch has sufficient free storage space for the upgrade file, as shown in Table 5.

Table 5 Minimum free storage space requirements

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.

Upgraded images	Minimum free storage space requirements
Boot ROM	Same size as the Boot ROM upgrade image file.

If no sufficient space is available, delete unused files as described in "Managing files from the Boot menu."

Scheduling the upgrade time

During the upgrade, the switch cannot provide any services. You must make sure the upgrade has a minimal impact on the network services.

Accessing the Boot menu

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU

********************************************************************************
*                                                                              *
*               HPE 5130-48G-4SFP+ EI Switch BOOTROM, Version 112               *
*                                                                              *
********************************************************************************
Copyright (c) 2010-2015 Hewlett-Packard Development Company, L.P.

Creation Date       : Apr 13 2015, 14:45:33
CPU Clock Speed     : 1000MHz
Memory Size         : 1024MB
Flash Size          : 512MB
CPLD Version        : 001
PCB Version         : Ver.B
Mac Address         : 443192f992f1

PEX mode is disabled.
Press Ctrl+B to access EXTENDED BOOT MENU...0
```

Press one of the shortcut key combinations at prompt.

Table 6 Shortcut keys

Shortcut keys	Prompt message	Function	Remarks
Ctrl+B	Press Ctrl+B to enter Extended Boot menu...	Accesses the extended Boot menu.	Press the keys within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the message appears. You can upgrade and manage system software and Boot ROM from this menu.

Shortcut keys	Prompt message	Function	Remarks
Ctrl+D	Press Ctrl+D to access BASIC BOOT MENU	Accesses the basic Boot menu.	Press the keys within 1 seconds after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.

Accessing the basic Boot menu

If the extended Boot ROM segment has corrupted, you can repair or upgrade it from the basic Boot menu.

Press **Ctrl+D** within 1 seconds after the "Press Ctrl+D to access BASIC BOOT MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended Boot ROM segment.

```
********************************************************************************
*                                                                              *
*                          BASIC BOOTROM, Version 112                          *
*                                                                              *
********************************************************************************

   BASIC BOOT MENU

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
4. Boot extended BootRom
0. Reboot
Ctrl+U: Access BASIC ASSISTANT MENU

Enter your choice(0-4):
```

Table 7 Basic Boot ROM menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
2. Update extended BootRom	Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
3. Update basic BootRom	Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.

Option	Task
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see Accessing the extended Boot menu.
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press **Ctrl + U** to access the BASIC ASSISTANT menu (see Table 8).

Table 8 BASIC ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.
0. Return to boot menu	Return to the basic Boot menu.

Accessing the extended Boot menu

Press **Ctrl+B** within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the "Press Ctrl-B to enter Extended Boot menu..." prompt message appears. If you fail to do this, the system starts decompressing the system software.

Alternatively, you can enter **4** in the basic Boot menu to access the extended Boot menu.

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 9). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 5130 EI Switch Series Configuration Guides*.

```
Password recovery capability is enabled.

EXTENDED BOOT MENU

      1. Download image to flash
      2. Select image to boot
      3. Display all files in flash
      4. Delete file from flash
      5. Restore to factory default configuration
      6. Enter BootRom upgrade menu
      7. Skip current system configuration
      8. Set switch startup mode
      0. Reboot
      Ctrl+Z: Access EXTENDED ASSISTANT MENU
      Ctrl+F: Format file system
      Ctrl+P: Change authentication for console login
      Ctrl+R: Download image to SDRAM and run
      Ctrl+Y: Change Work Mode
      Ctrl+C: Display Copyright

      Enter your choice(0-8):
```

Table 9 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	• Specify the main and backup software image file for the next startup. • Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+R: Download image to SDRAM and run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 10.
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

Table 10 EXTENDED ASSISTANT menu options

Option	Task
1. Display Memory	Display data in the memory.
2. Search Memory	Search the memory for a specific data segment.
0. Return to boot menu	Return to the extended Boot ROM menu.

Upgrading Comware images from the Boot menu

You can use the following methods to upgrade Comware images:

- Using TFTP to upgrade software images through the Ethernet port

- Using FTP to upgrade software images through the Ethernet port
- Using XMODEM to upgrade software through the console port

Using TFTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 11 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter **N**.

```
Loading.....................................................................
.............................................................................
.............................................................................
.....................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash...............................................................
.............................................................................
.....................................................Done!
```

```
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................Done!
```

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images are not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

Enter your choice(0-8): 0
```

Using FTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **2** to set the FTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
```

```
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
FTP User Name       :switch
FTP User Password   :***
```

Table 12 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter **N**.

```
Loading.....................................................................
.....................................................................
.....................................................................
.....................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash.....................................................................
.....................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
```

```
.....................................................................
.....................................................................Done!

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

Enter your choice(0-8):0
```

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

Using XMODEM to upgrade software through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **3** to set the XMODEM download baud rate.

```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
```

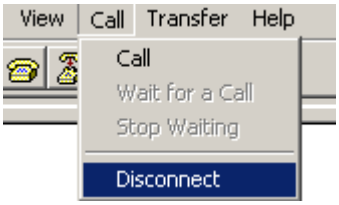
```
0.  Return to boot menu

Enter your choice(0-5):5
```

3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

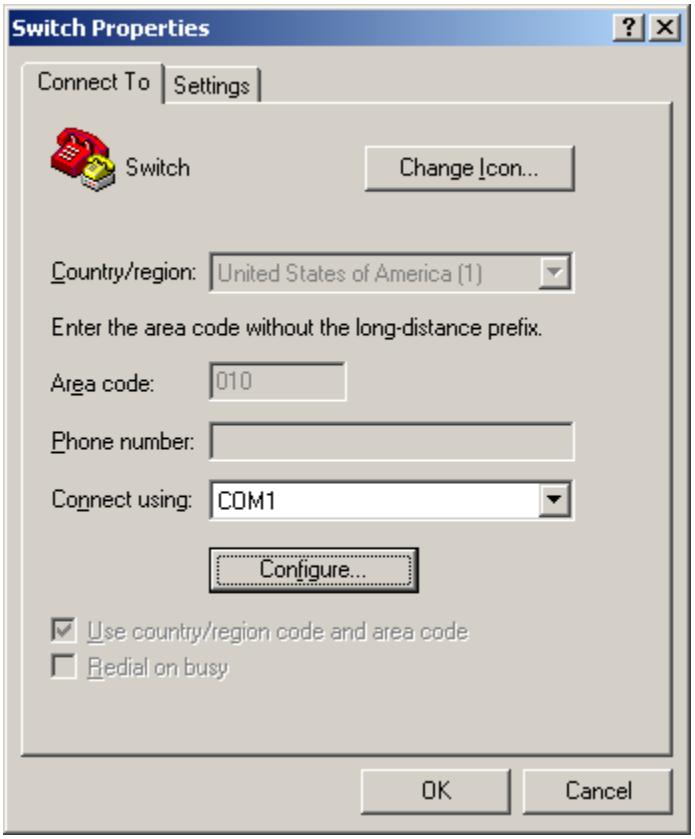
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



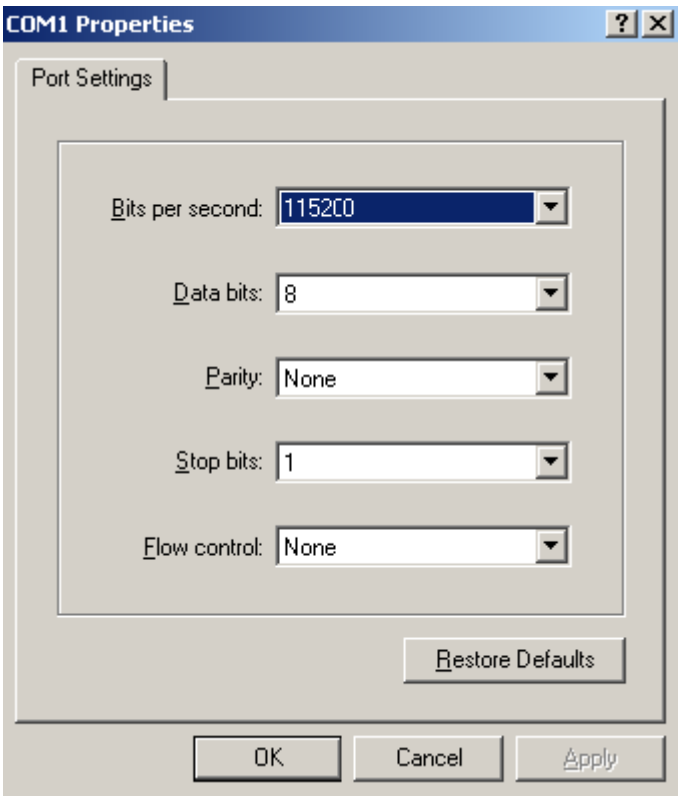
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



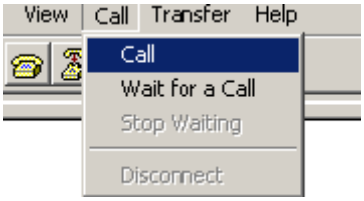
   c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 4 Modifying the baud rate



d. Select **Call** > **Call** to reestablish the connection.

Figure 5 Reestablishing the connection



5. Press **Enter**. The following prompt appears:

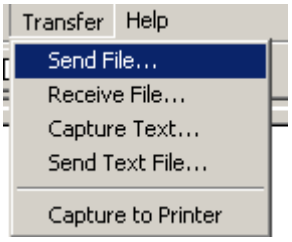
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC
```

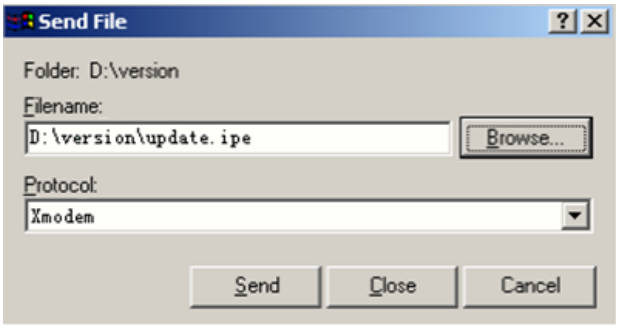
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 6 Transfer menu



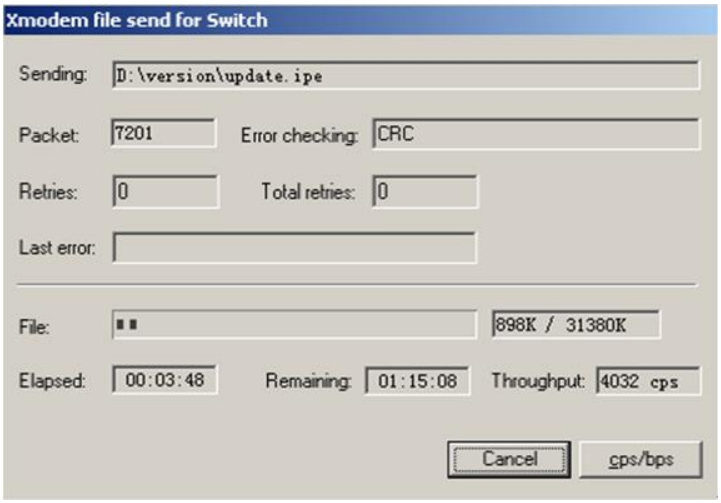
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box



9. Click **Send**. The following dialog box appears:

Figure 8 File transfer progress



10. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
```

At the **Load File name** prompt, enter a name for the boot image to be saved to flash memory.

```
Load File name  : default_file boot-update.bin       (At the prompt,
Free space: 470519808 bytes
Writing flash.....................................................................
.............Done!
The system-update.bin image is self-decompressing...
```

At the **Load File name** prompt, enter a name for the system image to be saved to flash memory.

```
Load File name  : default_file system-update.bin
Free space: 461522944 bytes
Writing flash.....................................................................
.............Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in the flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in flash memory, the attribute of the old image changes to none after the new image becomes valid.

11. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps as described in step 5.a. If the baud rate is 9600 bps, skip this step.

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright


Enter your choice(0-8): 0
```

12. Enter **0** in the Boot menu to reboot the system with the new software images.

Upgrading Boot ROM from the Boot menu

You can use the following methods to upgrade the Boot ROM image:

- Using TFTP to upgrade Boot ROM through the Ethernet port
- Using FTP to upgrade Boot ROM through the Ethernet port
- Using XMODEM to upgrade Boot ROM through the console port

Using TFTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
```

```
Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.btm
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 13 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.............................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom...........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using FTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **2** to set the FTP parameters.

```
Load File Name     :update.btm
Server IP Address  :192.168.0.3
Local IP Address   :192.168.0.2
Subnet Mask        :255.255.255.0
Gateway IP Address :0.0.0.0
FTP User Name      :switch
FTP User Password  :123
```

Table 14 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.............................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
```

```
Updating Basic BootRom..........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using XMODEM to upgrade Boot ROM through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **3** to set the XMODEM download baud rate.

```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

Enter your choice(0-5):5
```

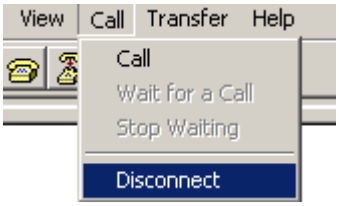
4. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

5. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.

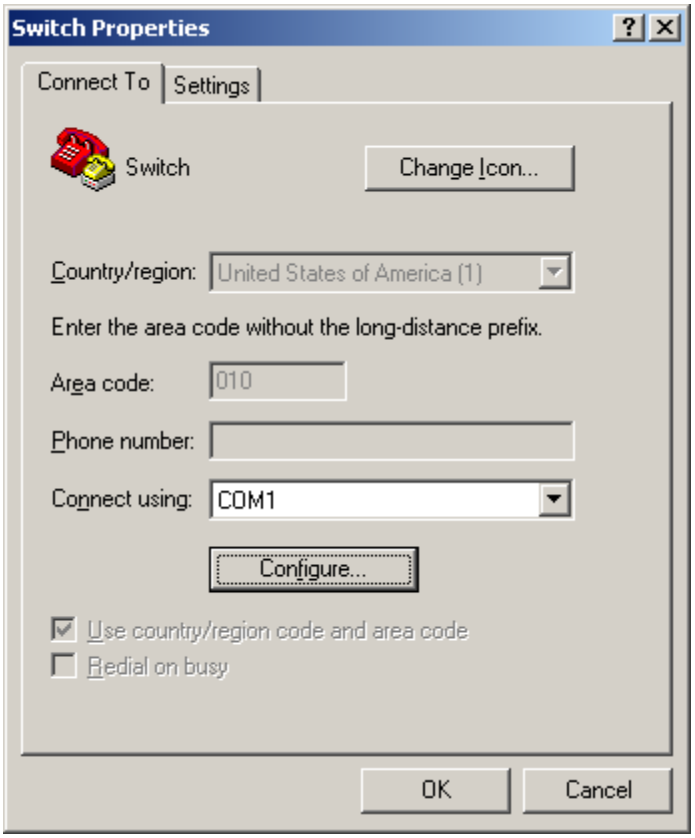
a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



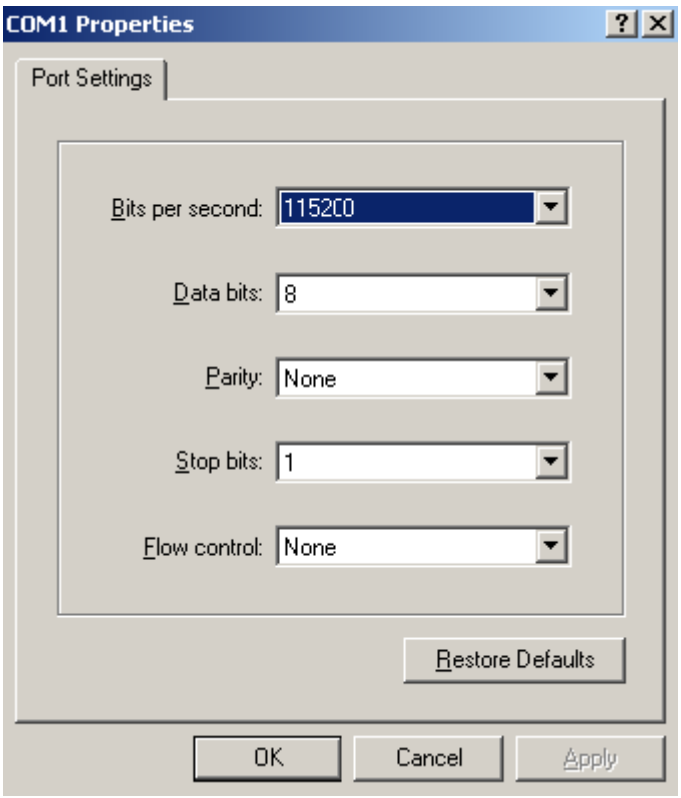
b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



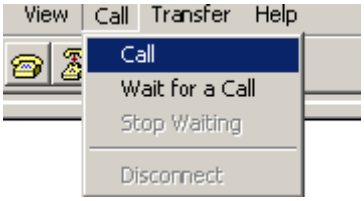
c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



d. Select **Call** > **Call** to reestablish the connection.

Figure 12 Reestablishing the connection

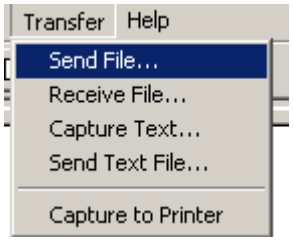


6. Press **Enter** to start downloading the file.

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC
```

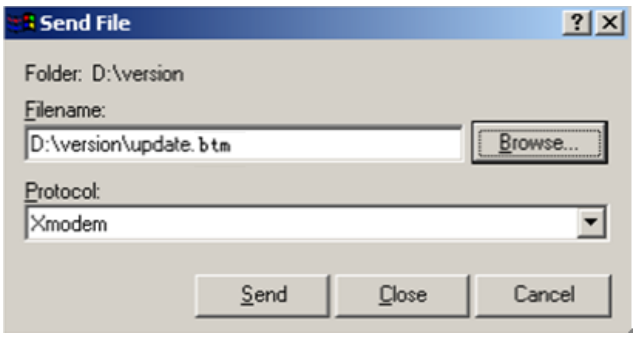
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



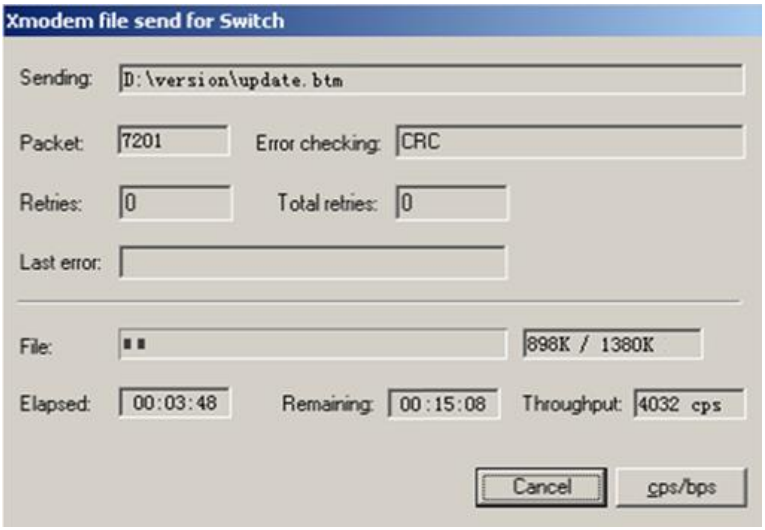
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 14 File transmission dialog box



9. Click **Send**. The following dialog box appears:

Figure 15 File transfer progress



10. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Loading ...CCCCCCCCCCCCCC  ...Done!
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

11. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

12. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps at the prompt, as described in step 4.a. If the baud rate is 9600 bps, skip this step.

```
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.
```

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

13. Press **Enter** to access the Boot ROM update menu.

14. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
```

```
0. Return to boot menu

Enter your choice(0-3):
```

15. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Managing files from the Boot menu

From the Boot menu, you can display files in flash memory to check for obsolete files, incorrect files, or space insufficiency, delete files to release storage space, or change the attributes of software images.

Displaying all files

Enter **3** in the Boot menu to display all files in flash memory and identify the free space size.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

    Enter your choice(0-8): 3
```

The following is a sample output:

```
Display all file(s) in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
4              3678                 flash:/startup.cfg_backup
5              30033                flash:/default.mdb
6              42424                flash:/startup.mdb
7              18                   flash:/.pathfile
8              232311               flash:/logfile/logfile.log
9              5981                 flash:/startup.cfg_back
10(*)          6098                 flash:/startup.cfg
11             20                   flash:/.snmpboots
Free space: 464298848 bytes
```

```
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

Deleting files

If storage space is insufficient, delete obsolete files to free up storage space.

To delete files:

1. Enter **4** in the Boot menu:

```
Deleting the file in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
4              3678                 flash:/startup.cfg_backup
5              30033                flash:/default.mdb
6              42424                flash:/startup.mdb
7              18                   flash:/.pathfile
8              232311               flash:/logfile/logfile.log
9              5981                 flash:/startup.cfg_back
10(*)          6098                 flash:/startup.cfg
11             20                   flash:/.snmpboots
Free space: 464298848 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

2. Enter the number of the file to delete. For example, enter **1** to select the file **testbackup.cfg**.

```
Please input the file number to change: 1
```

3. Enter **Y** at the confirmation prompt.

```
The file you selected is testbackup.cfg,Delete it? (Y/N):Y
Deleting.................................Done!
```

Changing the attribute of software images

Software image attributes include main (M), backup (B), and none (N). System software and boot software can each have multiple none-attribute images but only one main image and one backup image on the switch. You can assign both the M and B attributes to one image. If the M or B attribute you are assigning has been assigned to another image, the assignment removes the attribute from that image. If the removed attribute is the sole attribute of the image, its attribute changes to N.

For example, the system image **system.bin** has the M attribute and the system image **system-update.bin** has the B attribute. After you assign the M attribute to **system-update.bin**, the attribute of **system-update.bin** changes to M+B and the attribute of **system.bin** changes to N.

To change the attribute of a system or boot image:

1. Enter **2** in the Boot menu.

```
   EXTENDED BOOT MENU


1. Download image to flash
```

```
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

Enter your choice(0-8): 2
```

2. **1** or **2** at the prompt to set the attribute of a software image. (The following output is based on the option **2**. To set the attribute of a configuration file, enter **3**.)

```
1. Set image file
2. Set bin file
3. Set configuration file
0. Return to boot menu

Enter your choice(0-3): 2

File Number    File Size(bytes)     File Name
================================================================================

1(*)              53555200             flash:/system.bin
2(*)              9959424              flash:/boot.bin
3                 13105152             flash:/boot-update.bin
4                 91273216             flash:/system-update.bin
Free space: 417177920 bytes
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Note:Select .bin files. One but only one boot image and system image must be included.
```

3. Enter the number of the file you are working with. For example, enter 3 to select the boot image **boot-update.bin**. and enter **4** to select the system image **system-update.bin**.

```
Enter file No.(Allows multiple selection):3
Enter another file No.(0-Finish choice):4
```

4. Enter **0** to finish the selection.

```
Enter another file No.(0-Finish choice):0
You have selected:
flash:/boot-update.bin
flash:/system-update.bin
```

5. Enter **M** or **B** to change its attribute to main or backup. If you change its attribute to M, the attribute of **boot.bin** changes to none.

```
Please input the file attribute (Main/Backup) M
This operation may take several minutes. Please wait....
Next time, boot-update.bin will become default boot file!
Next time, system-update.bin will become default boot file!
Set the file attribute success!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version.

To handle a software upgrade failure:

1. Verify that the software release is compatible with the switch model and the correct file is used.
2. Verify that the software release and the Boot ROM release are compatible. For software and Boot ROM compatibility, see the hardware and software compatibility matrix in the correct release notes.
3. Check the physical ports for a loose or incorrect connection.
4. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
5. Check the file transfer settings:
   - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
   - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
   - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.
6. Check the FTP or TFTP server for any incorrect setting.
7. Check that the storage device has sufficient space for the upgrade file.

Hewlett Packard Enterprise

HPE 5130EI-CMW710-R3507P10 Release Notes Software Feature Changes

Contents

Release 3507P10

This release has no feature changes.

Release 3507P09

This release has no feature changes.

Release 3507P02

This release has no feature changes.

Release 3507

This release has the following changes:

- Modified feature: EAD assistant

Modified feature: EAD assistant

Feature change description

As from this version, you can use both EAD assistant and MAC authentication on the device.

Before modification: EAD assistant is mutually exclusive with MAC authentication and port security.

- You cannot enable EAD assistant when MAC authentication or port security is enabled globally.
- You cannot enable MAC authentication or port security globally when EAD assistant is enabled.

After modification: EAD assistant is still mutually exclusive with the port security feature, but you can use both EAD assistant and MAC authentication on the device. When you use both EAD assistant and MAC authentication on the device, follow these restrictions and guidelines:

- If both EAD assistant and MAC authentication are configured on the device, the MAC address of a user that fails MAC authentication is not marked as a silent MAC address. If the user has never passed MAC authentication, packets from the user can trigger MAC authentication again only after the user's EAD entry ages out.
- As a best practice, do not configure MAC authentication guest VLANs or critical VALNs. The VLANs might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- As a best practice, do not configure the Web authentication or IP source guard feature. The feature might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- If the MAC address of a user has been marked as a silent MAC address before EAD assistant is enabled, packets from the user can trigger 802.1X or MAC authentication only after the quiet timer expires.

Command changes

None.

Release 3506P10

This release has the following changes:

- New feature: Configuring the 802.1p priority for control packets sent by a device
- New feature: Packet spoofing logging and filtering entry logging for SAVI
- New feature: Configuring password control over weak passwords
- New feature: Enabling password change prompt logging

New feature: Configuring the 802.1p priority for control packets sent by a device

Configuring the 802.1p priority for control packets sent by a device

About this task

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

Restrictions and guidelines

This feature configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, ICMP, SSH, Telnet, RADIUS, SYSLOG, and SNMP.

Procedure

1. Enter system view.

   `system-view`
2. Configure the 802.1p priority for control packets sent by the device

   `control-packet dot1p` *`priority`*

   By default, the 802.1p priority is 6 for control packets sent by a device.

Command reference

control-packet dot1p

Use **`control-packet dot1p`** to configure the 802.1p priority for control packets sent by a device.

Use **`undo control-packet dot1p`** to restore the default.

Syntax

`control-packet dot1p` *`priority`*

`undo control-packet dot1p`

Default

The 802.1p priority is 6 for control packets sent by a device.

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

priority: Specifies an 802.1p priority value in the range of 0 to 7. 0 indicates the lowest priority, and 7 indicates the highest priority.

Usage guidelines

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

This command configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, ICMP, SSH, Telnet, RADIUS, SYSLOG, and SNMP. As a best practice, make sure you have known the impact on the network before executing this command.

Examples

Configure the 802.1p priority as 7 for control packets sent by the device.

```
<Sysname> system-view
[Sysname] control-packet dot1p 7
```

New feature: Packet spoofing logging and filtering entry logging for SAVI

Enabling packet spoofing logging and filtering entry logging

About this task

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.

   system-view

2. Enable packet spoofing logging.

   ipv6 savi log enable spoofing-packet [**interval** *interval* | **total-number** *number*] *

   By default, packet spoofing logging is disabled.

3. Enable filtering entry logging.

   ipv6 savi log enable filter-entry

   By default, filtering entry logging is disabled.

Command reference

ipv6 savi log enable

Use **ipv6 savi log enable** to enable packet spoofing logging or filtering entry logging.

undo ipv6 savi log enable to disable packet spoofing logging or filtering entry logging.

Syntax

ipv6 savi log enable { **spoofing-packet** [**interval** *interval* | **total-number** *number*] * | **filter-entry** }

undo ipv6 savi log enable { **spoofing-packet** | **filter-entry** }

Default

Packet spoofing logging and filtering entry logging are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

spoofing-packet [**interval** *interval* | **total-number** *number*]: Enables packet spoofing logging.

- **interval** *interval*: Sets the log output interval in seconds. The value of the *interval* argument can be 0 or in the range of 5 to 3600. The default value is 60 seconds. If you set this parameter to 0, the device outputs a log message immediately after it is generated.
- **total-number** *number*: Sets the maximum number of log messages that can be output per interval. The value range for the *number* argument is 1 to 128, and the default value is 128.

filter-entry: Enables filtering entry logging.

Usage guidelines

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see *Network Management and Monitoring Configuration Guide*.

The device can output a maximum of 128 packet spoofing log messages. If this limit is crossed, the device drops excess log messages. To ensure device performance, set the log output interval and maximum number of log messages output per interval appropriately.

Examples

Enable packet spoofing logging.

```
<Sysname> system-view
[Sysname] ipv6 savi log enable spoofing-packet
```

New feature: Configuring password control over weak passwords

Configuring password control over weak passwords

About this task

The system checks for weak passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

Procedure

1. Enter system view.

   `system-view`

2. Enable mandatory weak password change.

   `password-control change-password weak-password enable`

   By default, the mandatory weak password change feature is disabled.

Command reference

New command: password-control change-password weak-password enable

Use **`password-control change-password weak-password enable`** to enable mandatory weak password change.

Use **`undo password-control change-password weak-password enable`** to disable mandatory weak password change.

Syntax

`password-control change-password weak-password enable`

`undo password-control change-password weak-password enable`

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The system checks for weak login passwords for Telnet, SSH, HTTP, or HTTPS device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.

- Minimum password length restriction.
- Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

By default, the global composition policy and global minimum password length are as follows:

- A password must contain a minimum of two character types and a minimum of one character for each type.
- A password must contain a minimum of 10 characters.

By default, the password composition policy for a user group equals the global setting. The password composition policy for a local user equals that of the user group to which the local user belongs.

To change the password composition restriction and minimum password length, use the **password-control composition** and **password-control length** commands, respectively.

Examples

Enable the mandatory weak password change feature.

```
<Sysname> system-view
[Sysname] password-control change-password weak-password enable
```

Related commands

password-control { **aging** | **composition** | **history** | **length** } **enable**

password-control complexity

password-control composition

password-control length

password-control enable

Modified command: display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Predefined user roles

network-admin

Change description

Before modification: The **Password change** field does not contain the enabling state of the mandatory weak password change feature.

After modification: The **Password change** field displays the enabling state of the mandatory weak password change feature, including **Enabled (mandatory weak password change)** and **Disabled (mandatory weak password change)**.

Modified command: password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

After modification: By default, the global password complexity checking policy is as follows:

- In non-FIPS mode:

  The global password complexity checking policy is that username checking is enabled and repeated character checking is disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

- In FIPS mode:

  The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Modified command: password-control composition

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global composition policy requires that a password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, the global composition policy requires that a password must contain a minimum of two character types and a minimum of one character for each type.

Modified command: password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Views

System view

Change description

Before modification: By default, a super password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, a super password must contain a minimum of two character types and a minimum of one character for each type.

Modified command: set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Change description

Before modification: The password in plaintext form is a string of 1 to 16 characters.

After modification: The password in plaintext form is a string of 4 to 16 characters, and must contain a minimum of two character types and a minimum of one character for each type.

New feature: Enabling password change prompt logging

Enabling password change prompt logging

About this task

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the **password-control composition** command.
- Minimum password length restriction set by using the **password-control length** command.
- It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

Restrictions and guidelines

You can use the **display password-control** command to display password control configuration. For more information about password control commands, see password control commands in *Security Command Reference*.

Procedure

1. Enter system view.

   system-view
2. Enable password change prompt logging.

   local-server log change-password-prompt

   By default, password change prompt logging is enabled.

Command reference

local-server log change-password-prompt

Use **local-server log change-password-prompt** to enable password change prompt logging.

Use **undo local-server log change-password-prompt** to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature to enhance the protection of passwords for Telnet, SSH, HTTP, HTTPS, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the **password-control composition** command.
- Minimum password length restriction set by using the **password-control length** command.
- It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

You can use the **display password-control** command to display password control configuration. For more information about password control commands, see password control commands in *Security Command Reference*.

Examples

Enable password change prompt logging.

```
<Sysname> system-view
[Sysname] local-server log change-password-prompt
```

Related commands

display password-control

password-control composition

password-control length

Release 3506P08

This release has no feature changes.

Release 3506P06

This release has the following changes:

- New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device
- Modified feature: Factory defaults change for console login and password control settings

New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device

Enabling recording untrusted DHCP servers on a DHCP snooping device

About this task

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Procedure

1. Enter system view.

   system-view
2. Enable recording untrusted DHCP servers.

   dhcp snooping untrusted-server-record enable

   By default, the device does not record untrusted DHCP servers.

Command reference

dhcp snooping untrusted-server-record enable

Use **dhcp snooping untrusted-server-record enable** to enable recording untrusted DHCP servers.

Use **undo dhcp snooping untrusted-server-record enable** to disable recording untrusted DHCP servers.

Syntax

dhcp snooping untrusted-server-record enable

undo dhcp snooping untrusted-server-record enable

Default

Recording untrusted DHCP servers is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Examples

Enable the DHCP snooping device to record untrusted DHCP servers

```
<Sysname> system-view
[Sysname] dhcp snooping untrusted-server-record enable
```

Modified feature: Factory defaults change for console login and password control settings

Feature change description

Factory defaults are custom basic settings that came with the device. You can use the **display default-configuration** command to display factory defaults.

The device starts up with the factory defaults if no next-startup configuration files are available.

In this version, the following factory default settings are added:

```
#
password-control enable
#
local-user admin class manage
service-type terminal
authorization-attribute user-role network-admin
#
line class aux
authentication-mode scheme
#
undo password-control aging enable
#
undo password-control composition enable
#
undo password-control history enable
#
undo password-control length enable
```

```
#
password-control login idle-time 0
#
password-control login-attempt 3 exceed unlock
#
password-control update-interval 0
#
```

The output shows that the factory defaults for console login and password control settings change:

- The device performs local AAA authentication for console users. A console user must use the username **admin** without any password to log in to the device for the first time. The user role **network-admin** is assigned to the login console user.
- By default, the global password control and password change at first login are both enabled. Users must change the password at first login before they can access the system. The new password must contain a minimum of four different characters.
- The default maximum account idle time is 0 days. The system has no restriction for the account idle time.
- The default minimum password update interval is 0 hours. The system has no requirement for the password update interval.
- The default maximum number of consecutive login failures is 3. When console user fails the maximum number of login attempts, the console user can continue using this user account to make login attempts.
- After a console user modifies the password after first login, if you want to delete the default user account **admin**, make sure either of the following conditions are met before deleting the user account **admin**:
  - Another user account with the highest permissions exists.
  - The **`authentication-mode none`** command has been configured for AUX user lines.
- If you add or modify security configurations, make sure they do not conflict with the factory defaults or will not lead login failures. For more information about factory defaults, see configuration file management in *Fundamentals Configuration Guide* for the product. For more information about AAA authentication and password control, see *Security Configuration Guide.*
- After the global password control is enabled, the device generates an lauth.dat file to save the authentication and login information for local users.
  - If you execute the **`restore factory-default`** command in user view to restore the factory defaults, the lauth.dat file will be deleted. After the device reboots, you can use the username **admin** without any password to log in to the device, and you are required to change the password.
  - If you restore the factory defaults through **Restore to factory default configuration** on the boot menu, the lauth.dat file will not be deleted. After the device reboots, you must use the latest password to log in to the device.

Command changes

None.

Release 3506P02

This release has no feature changes.

Release 3506

This release has the following changes:

- New feature: Enabling recording user IP address conflicts
- New feature: LDRA on the DHCPv6 snooping device
- New feature: Enabling link flapping protection on an interface
- New feature: Controlling the status of guest VLAN reauthentication in MAC authentication
- New feature: Specifying the Telnet service port number
- New feature: Enabling the DHCPv6 relay agent to support Option 79
- New feature: Configuring resource monitoring
- New feature: Archiving configuration to a remote SCP server
- New feature: Setting the DSCP value for SNMP responses
- New feature: Specifying the NTP time-offset thresholds for log and trap outputs
- New feature: Specifying the SNTP time-offset thresholds for log and trap outputs
- New feature: Configuring Link-up delay timer
- New feature: Configuring an EAP profile
- New feature: Configuring 802.1X unauthenticated user aging
- New feature: Configuring MAC authentication unauthenticated user aging
- New feature: VLAN check bypass for the port security MAC move feature
- New feature: Strict intrusion protection
- New feature: Specifying the source IP address for outgoing SCP packets
- New feature: gRPC
- Modified feature: Specifying the HTTPS redirect listening port number
- Modified feature: Specifying startup images
- Modified feature: Automatic configuration
- Modified feature: Displaying ARP snooping entries
- Modified feature: Clearing ARP snooping entries
- Modified feature: Setting the DHCP server response timeout time for DHCP server switchover
- Modified feature: Automatic configuration
- Modified feature: Physical type of a combo interface
- Modified feature: Physical state change suppression
- Modified feature: MAC-to-VLAN entries
- Modified feature: Displaying the loop detection configuration and status
- Modified feature: Setting the 802.1p priority for IGMP messages
- Modified feature: Setting the 802.1p priority for MLD messages
- Modified feature: Displaying IPv4SG bindings
- Modified feature: Displaying IPv6SG bindings
- Modified feature: Displaying the MFF configuration for a VLAN
- Modified feature: Associating Track with application modules
- Modified feature: Configuring binding attributes for local users

New feature: Enabling recording user IP address conflicts

Enabling recording user IP address conflicts

About this task

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration in the information center, see the information center in *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.

   system-view

2. Enable recording user IP address conflicts.

   arp user-ip-conflict record enable

Command reference

arp user-ip-conflict record enable

Use **arp user-ip-conflict record enable** to enable recording user IP address conflicts.

Use **undo arp user-ip-conflict record enable** to disable recording user IP address conflicts.

Syntax

arp user-ip-conflict record enable

undo arp user-ip-conflict record enable

Default

Recording user IP address conflicts is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration, see the information center in *Network Management and Monitoring Configuration Guide*.

An IRF member device can generate a maximum of 10 user IP address conflict logs per second.

To display user IP address conflict records, use the **display arp user-ip-conflict record** command.

Examples

Enable recording user IP address conflicts.

```
<Sysname> system-view
[Sysname] arp user-ip-conflict record enable
```

Related commands

display arp user-ip-conflict record

display arp user-ip-conflict record

Use **display arp user-ip-conflict record** to display user IP address conflict records.

Syntax

display arp user-ip-conflict record [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays user IP address conflict records for the master device.

Usage guidelines

Each IRF member device can save a maximum of 200 user IP address conflict records.

If the maximum number is reached, a new record will override the earliest record.

Examples

Display all user IP address conflict records.

```
<Sysname> display arp user-ip-conflict record
IP address: 10.1.1.1
System time: 2018-02-02 11:22:29
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/2
New SVLAN/CVLAN: 100/2
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142

IP address: 10.1.1.2
System time: 2018-02-02 10:20:30
Conflict count: 1
Log suppress count: 0
Old interface: GigabitEthernet1/0/1
New interface: GigabitEthernet1/0/2
Old SVLAN/CVLAN: 100/--
New SVLAN/CVLAN: 100/--
Old MAC: 00e0-ca63-8141
New MAC: 00e0-ca63-8142
```

Table 1 Command output

Field	Description
IP address	IP address of a user.
System time	Time when the user IP address conflict occurred.
Conflict count	Number of times that conflicts for the IP address.
Log suppress count	Number of times that user IP address conflict logs are suppressed.
Old interface	Output interface in the old ARP entry.
New interface	Output interface in the new ARP entry.
Old SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the old ARP entry. This field displays hyphens (`--`) if the ARP entry does not belong to any outer VLAN or inner VLAN.
New SVLAN/CVLAN	ID of the outer VLAN or inner VLAN in the new ARP entry. This field displays hyphens (`--`) if the ARP entry does not belong to any outer VLAN or inner VLAN.
Old MAC	MAC address in the old ARP entry.
New MAC	MAC address in the new ARP entry.

Related commands

arp user-ip-conflict record enable

New feature: LDRA on the DHCPv6 snooping device

Enabling LDRA on the DHCPv6 snooping device

About LDRA on the DHCPv6 snooping device

Some DHCPv6 servers assign IPv6 addresses or prefixes to DHCPv6 clients only based on the Interface ID option in a Relay-Forward packet. If no DHCPv6 relay agent exists between DHCPv6 clients and such a DHCP server, the IPv6 address or prefix assignment based on the Interface ID option will fail.

To solve this problem, you can enable the lightweight DHCPv6 relay agent (LDRA) on the interface that receives DHCPv6 requests. The feature allows the interface to generate a Relay-Forward packet for a received DHCPv6 request and to insert the Interface ID option in the packet. After receiving the Relay-Forward packet, the DHCPv6 server can assign an IPv6 address or prefix based on the Interface ID option.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Enable LDRA on the interface.
   ipv6 dhcp snooping relay-agent enable
   By default, LDRA is disabled on the interface.

Command reference

ipv6 dhcp snooping relay-agent enable

Use **ipv6 dhcp snooping relay-agent enable** to enable LDRA on an interface.

Use **undo ipv6 dhcp snooping relay-agent enable** to disable LDRA on an interface.

Syntax

ipv6 dhcp snooping relay-agent enable [**trust**]

undo ipv6 dhcp snooping relay-agent enable [**trust**]

Default

By default, LDRA is disabled on the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

trust: Specifies the interface as a trusted interface. The device trusts the Relay-Forward packets received on the interface and forwards these packets to the DHCPv6 server. If you do not specify this keyword, the device drops the Relay-Forward packets received on this interface.

Usage guidelines

A network might have multiple cascaded lightweight DHCPv6 relay agents. As a best practice, do not specify the **trust** keyword if illegal Relay-Forward packets exist in the network.

Before you enable this feature, execute the **ipv6 dhcp snooping enable** command to enable DHCPv6 snooping. Otherwise, this feature does not take effect.

If this command and the **ipv6 dhcp snooping option interface-id enable** command are both executed, this command does not take effect.

Examples

Enable LDRA on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping relay-agent enable
```

New feature: Enabling link flapping protection on an interface

Enabling link flapping protection on an interface

About link flapping protection

Link flapping on an interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when interface status on the active link changes between **UP** and **DOWN**, traffic switches between active and standby links. To solve this problem, configure this feature on the interface.

With this feature enabled on an interface, when the interface goes down, the system enables link flapping detection. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Restrictions and guidelines

This feature takes effect only if it is configured in both the system view and interface view.

The **link-delay** and **port link-flap protect enable** commands are mutually exclusive on an Ethernet interface.

To bring up an interface that has been shut down by link flapping protection, execute the **undo shutdown** command.

In the **display interface** command output, the **Link-Flap DOWN** value of the **Current state** field indicates that the interface has been shut down by link flapping protection.

IRF physical interfaces also support this feature. However, this feature on IRF physical interfaces works differently from this feature on common Ethernet interfaces as follows:

- To avoid IRF physical link flapping, which will affect the IRF system stability, this feature is enabled by default on IRF physical interfaces and is not affected by the status of global link flapping protection.

- If the number of detected flaps on an IRF physical interface reaches or exceeds the link flapping detection threshold during the link flapping detection interval, the system displays prompt messages rather than shuts down the interface.

Procedure

1. Enter system view.
   system-view
2. Enable link flapping protection globally.
   link-flap protect enable
   By default, link flapping protection is disabled globally.
3. Enter Ethernet interface view.
   interface *interface-type interface-number*
4. Enable link flapping protection on the Ethernet interface.
   port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] *
   By default, link flapping protection is disabled on an Ethernet interface.

Command reference

display link-flap protection

Use **display link-flap protection** to display information about link flapping protection on an interface.

Syntax

display link-flap protection [**interface** *interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface type, the command displays information about link flapping protection on all interfaces.

interface-number: Specifies an interface number. If you do not specify an interface number, the command displays information about link flapping protection on all interfaces of the specified type.

Examples

Display information about link flapping protection on all interfaces.

```
<Sysname> display link-flap protection
Link-flap protection: Enabled
Interface            Link-flap  Status  Interval  Threshold
GE1/0/1              Enabled    Down    10        5
GE1/0/2              Disabled   N/A     --        --
```

Table 2 Command output

Field	Description
Link-flap protection	Status of global link flapping protection: • **Enabled**—Link flapping protection is enabled globally. • **Disabled**—Link flapping protection is disabled globally.
Link-flap	Status of link flapping protection on an interface: • **Enabled**—Link flapping protection is enabled on an interface. • **Disabled**—Link flapping protection is disabled on an interface.
Status	Status of an interface: • **Down**—The interface has been shut down by the link flapping protection feature. • **N/A**—The interface status is not affected by the link flapping protection feature.
Interval	Link flapping detection interval for an interface.
Threshold	Link flapping detection threshold for an interface.

Related commands

`link-flap protect enable`

`port link-flap protect enable`

link-flap protect enable

Use **`link-flap protect enable`** to enable link flapping protection globally.

Use **`undo link-flap protect enable`** to disable link flapping protection globally.

Syntax

`link-flap protect enable`

`undo link-flap protect enable`

Default

Link flapping protection is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Link flapping on any interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when the interface status on the active link changes between **UP** and **DOWN**, traffic switches between active and standby links. To solve this problem, execute this command.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Link flapping protection takes effect only when it is enabled in both system view and interface view.

Examples

Enable link flapping protection globally.

```
<Sysname> system-view
[Sysname] link-flap protect enable
```

Related commands

port link-flap protect enable

port link-flap protect enable

Use **port link-flap protect enable** to enable link flapping protection on an interface.

Use **undo port link-flap protect enable** to disable link flapping protection on an interface.

Syntax

port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] *

undo port link-flap protect enable [**interval** | **threshold**]

Default

Link flapping protection is disabled on an interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval: Specifies the link flapping detection interval in seconds. The value range for this argument is 10 to 60. The default value for this argument is 10.

threshold: Specifies the link flapping detection threshold in the range of 5 to 10. The default value for this argument is 5.

Usage guidelines

Link flapping protection takes effect only when it is enabled in both system view and interface view.

If you do not specify the **interval** *interval* or **threshold** *threshold* option when you execute the **port link-flap protect enable** command, the command uses the default settings.

If you specify the **interval** or **threshold** keyword when you execute the **undo port link-flap protect enable** command, the command restores the default setting for the keyword.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

To bring up an interface that has been shut down by link flapping protection, execute the **undo shutdown** command.

This command and the **link-delay** command are mutually exclusive on an Ethernet interface.

IRF physical interfaces also support this feature. However, this feature on IRF physical interfaces works differently from this feature on common Ethernet interfaces as follows:

- To avoid IRF physical link flapping, which will affect the IRF system stability, this feature is enabled by default on IRF physical interfaces and is not affected by the status of global link flapping protection.

- If the number of detected flaps on an IRF physical interface reaches or exceeds the link flapping detection threshold during the link flapping detection interval, the system displays prompt messages rather than shuts down the interface.

Examples

Enable link flapping protection on an interface. Set the link flapping detection interval to 10 seconds, and set the link flapping detection threshold to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-flap protect enable interval 10 threshold 5
```

Related commands

link-delay

link-flap protect enable

New feature: Controlling the status of guest VLAN reauthentication in MAC authentication

Enabling guest VLAN reauthentication in MAC authentication

Overview

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

In software versions earlier than R3503, guest VLAN reauthentication is enabled by default and cannot be disabled from the CLI.

As from version R3503, you can enable guest VLAN reauthentication by using the **mac-authentication guest-vlan re-authenticate** command or disable the feature by using the **undo** form of the command.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the **mac-authentication timer user-aging guest-vlan** *aging-time-value* command.

As a best practice, set the reauthentication interval to a value greater than 30 seconds if the number of concurrent MAC authentication users on a port is likely to exceed 300.

Configuration procedure

To enable the guest VLAN reauthentication feature of MAC authentication on a port:

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Enable the guest VLAN reauthentication feature of MAC authentication on the port.

   mac-authentication guest-vlan re-authenticate

   By default, the guest VLAN reauthentication feature of MAC authentication is enabled on a port.

Command reference

mac-authentication guest-vlan re-authenticate

Use **mac-authentication guest-vlan re-authenticate** to enable the guest VLAN reauthentication feature of MAC authentication on a port.

Use **undo mac-authentication guest-vlan re-authenticate** to disable the guest VLAN reauthentication feature of MAC authentication on a port.

Syntax

mac-authentication guest-vlan re-authenticate

undo mac-authentication guest-vlan re-authenticate

Default

The guest VLAN reauthentication feature of MAC authentication is enabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the **mac-authentication timer user-aging guest-vlan** *aging-time-value* command.

Examples

Enable the guest VLAN reauthentication feature of MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan re-authenticate
```

Related commands

display mac-authentication

mac-authentication guest-vlan

mac-authentication guest-vlan auth-period

mac-authentication timer

New feature: Specifying the Telnet service port number

Specifying the Telnet service port number

About specifying the Telnet service port number

You can specify the Telnet service port number. By default, the Telnet service port number is 23.

Procedure

1. Enter system view.
   system-view
2. Specify the Telnet service port number.
   IPv4:
   telnet server port *port-number*
   IPv6:
   telnet server ipv6 port *port-number*

Command reference

telnet server ipv6 port

Use **telnet server ipv6 port** to specify the IPv6 Telnet service port number.

Use **undo telnet server ipv6 port** to restore the default.

Syntax

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv6 Telnet service port number to 1026.

```
<Sysname> system-view
[Sysname] telnet server ipv6 port 1026
```

telnet server port

Use **telnet server port** to specify the IPv4 Telnet service port number.

Use **undo telnet server port** to restore the default.

Syntax

telnet server port *port-number*

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv4 Telnet service port number to 1025.

```
<Sysname> system-view
[Sysname] telnet server port 1025
```

New feature: Enabling the DHCPv6 relay agent to support Option 79

Enabling the DHCPv6 relay agent to support Option 79

About enabling the DHCPv6 relay agent to support Option 79

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Enable the DHCPv6 relay agent to support Option 79.
   ipv6 dhcp relay client-link-address enable

By default, the DHCPv6 relay agent does not support Option 79.

Command reference

ipv6 dhcp relay client-link-address enable

Use **ipv6 dhcp relay client-link-address enable** to enable the DHCPv6 relay agent to support Option 79.

Use **undo ipv6 dhcp relay client-link-address enable** to disable Option 79 support.

Syntax

ipv6 dhcp relay client-link-address enable

undo ipv6 dhcp relay client-link-address enable

Default

The DHCPv6 relay agent does not support Option 79.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Examples

Enable Option 79 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay client-link-address enable
```

New feature:Enable recording DHCPv6 snooping prefix entries

Enable recording DHCPv6 snooping prefix entries

Restrictions and guidelines

If the basic DHCPv6 snooping features are configured globally, you can only use the undo form of the global configuration commands to disable the settings globally. The VLAN-specific configuration commands cannot disable the settings.

If the basic DHCPv6 snooping features are configured in a VLAN, you can only use the undo form of the VLAN-specific configuration commands to disable the settings in the VLAN. The global configuration command cannot disable the settings.

Procedure

Enter system view.

system-view

1. Enable DHCPv6 snooping globally.

   ipv6 dhcp snooping enable

   By default, DHCPv6 snooping is disabled globally.
2. Enter interface view.

   interface *interface-type interface-number*

   This interface must connect to the DHCPv6 server.
3. Specify the port as a trusted port.

   ipv6 dhcp snooping trust

   By default, all ports are untrusted ports after DHCPv6 snooping is enabled.
4. Enable recording DHCPv6 snooping entries.
   a. Return to system view.

      quit
   b. Enter interface view.

      interface *interface-type interface-number*

      This interface must connect to the DHCPv6 client.
   c. Enable recording DHCPv6 snooping prefix entries.

      ipv6 dhcp snooping pd binding record

      By default, recording of DHCPv6 snooping prefix entries is disabled.

Command reference

ipv6 dhcp snooping pd binding record

Use **ipv6 dhcp snooping pd binding record** to enable recording DHCPv6 snooping prefix entries.

Use **undo ipv6 dhcp snooping pd binding record** to disable recording DHCPv6 snooping prefix entries.

Syntax

ipv6 dhcp snooping pd binding record

undo ipv6 dhcp snooping pd binding record

Default

Recording of DHCPv6 snooping prefix entries is disabled.

Views

Layer 2 Ethernet interface/Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCPv6 snooping to record IPv6 prefix-to-port information of the DHCPv6 clients (called DHCPv6 snooping prefix entries). When IP source guard (IPSG) is configured on the DHCP snooping device, IPSG can generate dynamic bindings based on the DHCP snooping prefix entries to filter out illegitimate packets.

Examples

Enable DHCPv6 snooping prefix entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname]interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping pd binding record
```

Related commands

display ipv6 dhcp snooping pd binding

display ipv6 dhcp snooping pd binding

Use **display ipv6 dhcp snooping pd binding** to display DHCPv6 snooping prefix entries.

Syntax

display ipv6 dhcp snooping pd binding [**prefix** *prefix/prefix-length* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix *prefix/prefix-length*: Specifies an IPv6 prefix with its length. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Specifies the ID of the VLAN where the IPv6 prefix resides. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command takes effect only after you execute the **ipv6 dhcp snooping pd binding record** command on the port directly connecting to the clients.

If you do not specify any parameters, this command displays all DHCPv6 snooping prefix entries.

Examples

Display all DHCPv6 snooping prefix entries.

```
<Sysname> display ipv6 dhcp snooping pd binding
1 DHCPv6 snooping PD entries found.
IPv6 prefix      Lease       VLAN SVLAN Interface
================ =========== ==== ===== ========================
1:2::/64         54          2    N/A   GigabitEthernet1/0/1
```

Table 3 Command output

Field	Description
n DHCPv6 snooping PD entries found.	Total number of DHCPv6 snooping prefix entries.
IPv6 prefix	IPv6 prefix assigned to the DHCPv6 client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag.

Field	Description
	Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides.
SVLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.
Interface	Port connecting to the DHCPv6 client.

Related commands

ipv6 dhcp snooping pd binding record

reset ipv6 dhcp snooping pd binding

reset ipv6 dhcp snooping pd binding

Use **reset ipv6 dhcp snooping pd binding** to clear DHCPv6 snooping prefix entries.

Syntax

reset ipv6 dhcp snooping pd binding { **all** | **prefix** *prefix/prefix-length* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCPv6 snooping prefix entries.

prefix *prefix/prefix-length*: Clears DHCPv6 snooping entries for the specified IPv6 prefix. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Clears DHCPv6 snooping prefix entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command clears all DHCPv6 snooping prefix entries.

Examples

Clear DHCPv6 snooping prefix entries for 1:2::/64.

```
<Sysname> reset ipv6 dhcp snooping pd binding prefix 1:2::/64
```

Related commands

display ipv6 dhcp snooping pd binding

New feature: Configuring resource monitoring

About resource monitoring

The resource monitoring feature enables the device to monitor the available amounts of types of resources, for example, the space for ARP entries. The device samples the available amounts periodically and compares the samples with resource depletion thresholds to identify the resource depletion status.

The device supports a minor resource depletion threshold and a severe resource depletion threshold for each supported resource type.

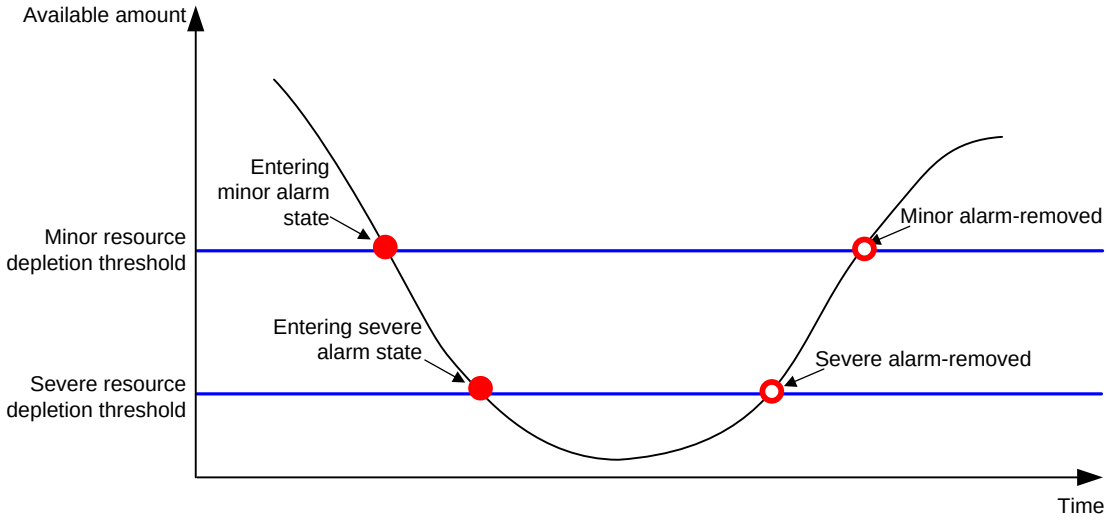
- If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
- If the available amount is equal to or less than the severe resource depletion threshold, the resource type is in severe alarm state.
- If the available amount increases above the minor resource depletion threshold, the resource type is in recovered state.

When a resource type enters severe alarm state, the device issues a severe alarm. If the resource type stays in severe alarm state, the device resends severe alarms periodically.

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

Resource depletion alarms can be sent to NETCONF, SNMP, and the information center to be encapsulated as NETCONF events, SNMP traps and informs, and log messages. For more information, see NETCONF, SNMP, and information center in *Network Management and Monitoring Configuration Guide*.

Figure 1 Resource depletion alarms and alarm-removed notifications



Procedure

1. Enter system view.

   system-view

2. Set resource depletion thresholds.

   resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

   The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

3. Specify destinations for resource depletion alarms.

   resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

By default, resource depletion alarms are sent to NETCONF, SNMP, and the information center.

4. Enable resending of minor resource depletion alarms.

   resource-monitor minor resend enable

   By default, resending of minor resource depletion alarms is enabled.

Command reference

resource-monitor minor resend enable

Use **resource-monitor minor resend enable** to enable resending of minor resource depletion alarms.

Use **undo resource-monitor minor resend enable** to disable resending of minor resource depletion alarms.

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend enable

Default

Resending of minor resource depletion alarms is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

The resending period is fixed at 24 hours for a severe alarm and is fixed at 7 * 24 hours for a minor alarm.

Examples

Enable resending of minor resource depletion alarms.

```
<Sysname> system-view
[Sysname] resource-monitor minor resend enable
```

Related commands

display resource-monitor

resource-monitor output

resource-monitor resource

resource-monitor output

Use **resource-monitor output** to specify destinations for resource depletion alarms.

Use **undo resource-monitor output** to remove destinations for resource depletion alarms.

Syntax

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

undo resource-monitor output [**netconf-event** | **snmp-notification** | **syslog**] *

Default

Resource depletion alarms are sent to NETCONF, SNMP, and the information center.

Views

System view

Predefined user roles

network-admin

Parameters

netconf-event: Sends resource depletion alarms to the NETCONF feature to encapsulate the alarms in NETCONF events. For more information, see NETCONF in *Network Management and Monitoring Configuration Guide*.

snmp-notification: Sends resource depletion alarms to the SNMP feature to encapsulate the alarms in SNMP traps and informs. For more information, see SNMP in *Network Management and Monitoring Configuration Guide*.

syslog: Sends resource depletion alarms to the information center to encapsulate the alarms in log messages. For more information, see information center in *Network Management and Monitoring Configuration Guide*.

Usage guidelines

If you do not specify any keywords for the **undo resource-monitor output** command, the command disables resource depletion alarm output.

Examples

Specify the information center module as the output destination for resource depletion alarms.

```
<Sysname> system-view
[Sysname] resource-monitor output syslog
```

Related commands

resource-monitor minor resend enable

resource-monitor resource

resource-monitor resource

Use **resource-monitor resource** to set resource depletion thresholds.

Use **undo resource-monitor resource** to disable resource depletion thresholds.

Syntax

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

Default

The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

Views

System view

Predefined user roles

network-admin

Parameters

resource-name: Specifies a resource type by its name. The values for this argument are case insensitive and cannot be abbreviated. Table 4 shows the resource types that can be monitored.

Table 4 Resource types that can be monitored

Resource type	Description
agg_group	Aggregation group hardware resources.
mac	MAC address table hardware resources.
mqcin	Inbound MQC resources.
mqcout	Outbound MQC resources.
mqcvlan	VFP MQC resources.
pfilterin	Inbound packet filter resources.
pfilterout	Outbound packet filter resources.

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

by-absolute: Specifies resource depletion thresholds by using absolute values.

by-percent: Specifies resource depletion thresholds in percentage.

minor-threshold *minor-threshold*: Specifies the minor resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *minor-threshold* argument.

severe-threshold *severe-threshold*: Specifies the severe resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *severe-threshold* argument.

Usage guidelines

After you execute this command for a resource type, the device monitors the available amount of the type of resources. The device samples the available amount at intervals, compares the sample with the resource depletion thresholds to identify the resource depletion status, and sends alarms as configured.

Examples

Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for ARP entry resources on slot 1.

```
<Sysname> system-view
[Sysname] resource-monitor resource arp slot 1 cpu 0 by-percent minor-threshold 30
severe-threshold 10
```

Related commands

display resource-monitor

resource-monitor minor resend enable

resource-monitor output

display resource-monitor

Use **display resource-monitor** to display resource monitoring information.

Syntax

display resource-monitor [**resource** *resource-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource *resource-name*: Specifies a resource type by its name. For information about available resource types, see Table 4.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays resource monitoring information for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display ARP resource monitoring information.

```
<Sysname> display resource-monitor resource arp
Minor alarms resending: Enabled

Slot 1:
Resource                        Minor Severe Free/Total
                                (%)   (%)    (absolute)
arp                             50    20     90095/90098
```

Table 5 Command output

Field	Description
Minor alarms resending	Status of the minor resource depletion alarm resending feature, **Enabled** or **Disabled.**
Resource	Monitored resource type.
Minor (%)	Minor resource depletion threshold, in percentage.
Severe (%)	Severe resource depletion threshold, in percentage.
Free/Total (absolute)	Numbers of available resources and total resources, in absolute values.

Related commands

resource-monitor minor resend enable

resource-monitor resource

New feature: Archiving configuration to a remote SCP server

Configuring remote configuration archiving

About remote configuration archiving

As from this version, the device supports archiving the running configuration to a remote SCP server.

Before archiving the running configuration, you must set a file directory and file name prefix for configuration archives. The archive directory is located on a remote SCP server.

Configuration archives are named in the format of *prefix_YYYYMMDD_HHMMSS***.cfg**, for example, **archive_20170526_203430.cfg**.

If you change the file directory or file name prefix on the remote SCP server, the **display archive configuration** command no longer displays the old configuration archives saved before the change.

Restrictions and guidelines

Remote archiving (the **archive configuration server** command) and local archiving (the **archive configuration location** command) are mutually exclusive. You cannot use the two features at the same time.

IMPORTANT:

In FIPS mode, the device does not support archiving the running configuration to a remote SCP server.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the **archive configuration max** command.

The **undo archive configuration server** command removes the remote configuration archive directory and file name prefix settings, but it does not delete the configuration archives on the server. The command also performs the following operations:

- Disables both the manual and automatic configuration archiving features.
- Restores the default setting for the **archive configuration interval** command.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Procedure

1. Enter system view.

   system-view

2. Set the directory and file name prefix for archiving the running configuration on a remote SCP server.

   archive configuration server scp { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**directory** *directory*] **filename-prefix** *filename-prefix*

   By default, no path or file name prefix is set for archiving the running configuration to a remote SCP server.

3. Configure the username and password for accessing the remote SCP server:

   a. Configure the username.

archive configuration server user *user-name*

By default, no username is configured for accessing the SCP server.

b. Configure the password.

archive configuration server password { **cipher** | **simple** } *string*

By default, no password is configured for accessing the SCP server.

Make sure the username and password are the same as the SCP account settings on the SCP server.

Command reference

archive configuration server

Use **archive configuration server** to configure the parameters for archiving the running configuration to a remote SCP server.

Use **undo archive configuration server** to restore the default.

Syntax

archive configuration server scp { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**directory** *directory*] **filename-prefix** *filename-prefix*

undo archive configuration server

Default

No parameters are set for archiving the running configuration to a remote SCP server.

Views

System view

Predefined user roles

network-admin

Parameters

scp: Specifies a remote SCP server.

ipv4-address: Specifies the SCP server by its IPv4 address.

ipv6 *ipv6-address*: Specifies the SCP server by its IPv6 address.

port *port-number*: Specifies the TCP port number of the SCP server.

directory *directory*: Specifies the archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the SCP server.

filename-prefix *filename-prefix*: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

IMPORTANT:

In FIPS mode, the device does not support archiving the running configuration to a remote SCP server.

Before archiving the running configuration to a remote SCP server, you must perform the following tasks:

- Use this command to specify a configuration archive directory and a name prefix on the remote SCP server.
- Use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

To manually archive the running configuration, use the **archive configuration** command. To periodically archive the running configuration, use the **archive configuration interval** command.

On the specified remote SCP server, configuration archives are named in the format of *filename-prefix*_YYYYMMDD_HHMMSS**.cfg**, for example, **archive_20170526_203430.cfg**.

Local archiving (the **archive configuration location** command) and remote archiving (the **archive configuration server** command) are mutually exclusive. You cannot use the two features at the same time.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the **archive configuration max** command.

The **undo archive configuration server** command removes the configuration archive directory and file name prefix settings, but it does not delete the configuration archives saved on the server. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default setting for the **archive configuration interval** command.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **archive/** on the SCP server at 192.168.1.1 and set the archive file name prefix as **my_archive**.

```
<Sysname> system-view
[Sysname] archive configuration server scp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

archive configuration server password

Use **archive configuration server password** to configure the password for accessing the SCP server that saves configuration archives.

Use **undo archive configuration server password** to restore the default.

Syntax

archive configuration server password { **cipher** | **simple** } *string*

undo archive configuration server password

Default

No password is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the SCP server that saves configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server password simple admin
```

Related commands

archive configuration server

archive configuration server user

display archive configuration

archive configuration server user

Use **archive configuration server user** to configure the username for accessing the SCP server that saves configuration archives.

Use **undo archive configuration server user** to restore the default.

Syntax

archive configuration server user *user-name*

undo archive configuration server user

Default

No username is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

Set the username to **admin** for accessing the SCP server that saves configuration archives.

```
<Sysname> system-view
```

```
[Sysname] archive configuration server user admin
```

Related commands

archive configuration server

archive configuration server password

display archive configuration

New feature: Setting the DSCP value for SNMP responses

Setting the DSCP value for SNMP responses

1. Enter system view.
   system-view
2. Set the DSCP value for SNMP responses.
   snmp-agent packet response dscp *dscp-value*
   By default, the DSCP value for SNMP responses is 0.

Command reference

snmp-agent packet response dscp

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP responses is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP responses, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 40 for SNMP responses.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 40
```

New feature: Specifying the NTP time-offset thresholds for log and trap outputs

Specifying the NTP time-offset thresholds for log and trap outputs

About the NTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the NTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Procedure

1. Enter system view.

   system-view

2. Specify the NTP time-offset thresholds for log and trap outputs.

   ntp-service time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

   By default, no NTP time-offset thresholds are set for log and trap outputs.

Command reference

ntp-service time-offset-threshold

Use **ntp-service time-offset-threshold** to set the NTP time-offset thresholds for log and trap outputs.

Use **undo ntp-service time-offset-threshold** to restore the default.

Syntax

ntp-service time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

undo ntp-service time-offset-threshold

Default

No NTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

log *log-threshold*: Specifies the NTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

trap *trap-threshold*: Specifies the NTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Set the NTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] ntp-service time-offset-threshold log 500 trap 600
```

New feature: Specifying the SNTP time-offset thresholds for log and trap outputs

Specifying the SNTP time-offset thresholds for log and trap outputs

About SNTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the SNTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Procedure

1. Enter system view.

   system-view

2. Specify the SNTP time-offset thresholds for log and trap outputs.

   sntp time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

   By default, no SNTP time-offset thresholds are set for log and trap outputs

Command reference

sntp time-offset-threshold

Use **sntp time-offset-threshold** to specify the SNTP time-offset thresholds for log and trap outputs.

Use **undo sntp time-offset-threshold** to restore the default.

Syntax

sntp time-offset-threshold { **log** *log-threshold* | **trap** *trap-threshold* } *

undo sntp time-offset-threshold

Default

No SNTP time-offset thresholds are set for log and trap outputs.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

log *log-threshold*: Specifies the SNTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

trap *trap-threshold*: Specifies the SNTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

Usage guidelines

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

Examples

Set the SNTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
[Sysname] sntp time-offset-threshold log 500 trap 600
```

New feature: Configuring Link-up delay timer

Configuring Link-up delay timer

About 802.1X unauthenticated user aging

This feature prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states. This feature behaves differently depending on whether you specify the **distribute** keyword in the **linkup-delay-timer** command.

- If you do not specify the **distribute** keyword, the master node starts the link-up delay timer when a faulty port comes up and the master node receives Hello packets from the secondary port.
  - If the master node can still receive Hello packets from the secondary port after the link-up delay timer expires, the master node performs the following operations:
    - Changes the RRPP ring state from Disconnect to Health.
    - Switches the traffic from the secondary port to the primary port.
  - If the master node cannot receive Hello packets from the secondary port after the Fail timer expires and before the link-up delay timer expires, the master node performs the following operations:
    - Stops the link-up delay timer.
    - Keeps the RRPP ring in Disconnect state.
- If you specify the **distribute** keyword, all nodes in the RRPP domain can learn the value of the link-up delay timer through Hello packets. When the faulty port comes up, the master node performs the following operations:
  - The hosting RRPP node blocks the faulty port (the faulty port cannot send or receive any packets).
  - Starts the link-up delay timer.

If the port does not become faulty after the link-up delay timer expires, the hosting RRPP node sets the port state to up. The master node can receive Hello packets from its secondary port again. Then, the master node changes the RRPP ring state from Disconnect to Health and switches the traffic from the secondary port to the primary port.

If the port becomes faulty again before the link-up delay timer expires, the hosting RRPP node blocks the port and stops the link-up delay timer.

Restrictions and guidelines

If the **distribute** keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

If you specify the **distribute** keyword in an RRPP network implementing load balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

Procedure

1. Enter system view.

   system-view

2. Enter RRPP domain view.

   rrpp domain *domain-id*

3. Set the link-up delay timer for the RRPP domain.

   linkup-delay-timer *delay-time* [**distribute**]

   By default, the link-up delay timer value is 0 seconds, and the **distribute** keyword is not specified.

Command reference

linkup-delay-timer

Use **linkup-delay-timer** to set the link-up delay timer.

Use **undo linkup-delay-timer** to restore the default.

Syntax

linkup-delay-timer *delay-time* [**distribute**]

undo linkup-delay-timer

Default

The link-up delay timer is 0 seconds, and the **distribute** keyword is not specified.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the link-up delay timer in the range of 0 to 30 seconds.

distribute: Enables all nodes in the RRPP domain to learn the link-up delay timer value.

Usage guidelines

The link-up delay timer prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states.

You can configure this command on any node in an RRPP domain, but this command can take effect only on the master node.

If you specify the **distribute** keyword in an RRPP network implementing loading balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

If the **distribute** keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

Examples

Set the link-up delay timer to 10 seconds for RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] linkup-delay-timer 10
```

Related commands

timer

New feature: Configuring an EAP profile

Configuring an EAP profile

About EAP profiles

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods.

Restrictions and guidelines

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Prerequisites

Before you specify a CA certificate file, use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

Procedure

1. Enter system view.

   system-view

2. Create an EAP profile and enter EAP profile view.

   eap-profile *eap-profile-name*

3. Specify the EAP authentication method.

   method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

   By default, the EAP authentication method is MD5-challenge.

4. Specify a CA certificate file for EAP authentication.

   ca-file *file-name*

   By default, no CA certificate file is specified for EAP authentication.

   You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Command reference

eap-profile

Use **eap-profile** to create an EAP profile and enter its view, or enter the view of an existing EAP profile.

Use **undo eap-profile** to delete an EAP profile.

Syntax

eap-profile *eap-profile-name*

undo eap-profile *eap-profile-name*

Default

No EAP profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

eap-profile-name: Specifies the EAP profile name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods. You can use an EAP profile in a test profile for RADIUS server status detection.

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Examples

Create an EAP profile named **eap1** and enter its view.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1]
```

Related commands

radius-server test-profile

ca-file

Use **ca-file** to specify a CA certificate file for EAP authentication.

Use **undo ca-file** to restore the default.

Syntax

ca-file *file-name*

undo ca-file

Default

No CA certificate file is specified for EAP authentication. The device does not verify the RADIUS server certificate during EAP authentication.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

file-name: Specifies a CA certificate file by its name, a case-sensitive string of 1 to 91 characters.

Usage guidelines

You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Before you specify a CA certificate file, you must use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

You can specify only one CA certificate file in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the CA certificate file, the new CA certificate file takes effect at the next server status detection.

Examples

In EAP profile **eap1**, specify CA certificate file **CA.der** for EAP authentication.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] ca-file CA.der
```

method

Use **method** to specify the EAP authentication method.

Use **undo method** to restore the default.

Syntax

method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo method

Default

MD5-challenge authentication is used.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge method.

peap-gtc: Specifies the PEAP-GTC method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 method.

ttls-gtc: Specifies the TTLS-GTC method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 method.

Usage guidelines

You must specify an EAP authentication method that is supported by the RADIUS server to be detected.

You can specify only one EAP authentication method in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the EAP authentication method, the new method takes effect in the next server status detection.

Examples

In EAP profile **eap1**, specify PEAP-GTC as the EAP authentication method.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] method peap-gtc
```

New feature: Configuring 802.1X unauthenticated user aging

Configuring 802.1X unauthenticated user aging

About 802.1X unauthenticated user aging

802.1X unauthenticated user aging applies to users added to an 802.1X guest, critical, or Auth-Fail VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

The 802.1X user aging mechanism on a port depends on its access control mode.

- If the port uses port-based access control, a user aging timer starts when the port is assigned to the critical or Auth-Fail VLAN. When the aging timer expires, the port is removed from the VLAN and all MAC address entries for users in the VLAN are also removed.
- If the port uses MAC-based access control, a user aging timer starts for each 802.1X user when they are assigned to the Auth-Fail, critical, or guest VLAN. When the aging timer for a user expires, the device removes that user from the VLAN.

The removed users will be unable to access any network resources until after another authentication is triggered.

Restrictions and guidelines

As a best practice, use this feature on a port only if you want to have its unauthenticated users to be authenticated and come online on a different port.

Procedure

1. Enter system view.

   system-view

2. Set the user aging timer for a type of 802.1X VLAN.

   dot1x timer user-aging { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } *aging-time-value*

By default, the user aging timers for all applicable types of 802.1X VLANs are 1000 seconds.

3. Enter interface view.

   interface *interface-type interface-number*

4. Enable 802.1X unauthenticated user aging.

   dot1x unauthenticated-user aging enable

   By default, 802.1X unauthenticated user aging is enabled.

Command reference

dot1x unauthenticated-user aging enable

Use **dot1x unauthenticated-user aging enable** to 802.1X unauthenticated user aging.

Use **undo dot1x unauthenticated-user aging enable** to disable 802.1X unauthenticated user aging.

Syntax

dot1x unauthenticated-user aging enable

undo dot1x unauthenticated-user aging enable

Default

User aging is enabled for 802.1X users that have not been authenticated or have not passed authentication.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

802.1X unauthenticated user aging applies to users added to 802.1X guest, critical, or Auth-Fail VLANs because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

The 802.1X user aging mechanism on a port depends on its access control mode.

- If the port uses port-based access control, a user aging timer starts when the port is assigned to the critical or Auth-Fail VLAN. When the aging timer expires, the port is removed from the VLAN and all MAC address entries for users in the VLAN are also removed.
- If the port uses MAC-based access control, a user aging timer starts for each 802.1X user when they are assigned to the Auth-Fail, critical, or guest VLAN. When the aging timer for a user expires, the device removes that user from the VLAN.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

The removed users will be unable to access any network resources until after another authentication is triggered.

Examples

Disable 802.1X user aging on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x unauthenticated-user aging enable
```

Related commands

dot1x timer

dot1x timer user-aging

Use **dot1x timer user-aging** to set the user aging timer for a type of 802.1X VLAN.

Use **undo dot1x timer user-aging** to restore the default user aging timer setting for a type of 802.1X VLAN.

Syntax

dot1x timer user-aging { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } *aging-time-value*

undo dot1x timer user-aging { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** }

Default

By default, the user aging timers for all applicable types of 802.1X VLANs are 1000 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

user-aging: Sets the user aging timer for a type of 802.1X VLAN.

auth-fail-vlan: Specifies 802.1X Auth-Fail VLANs.

critical-vlan: Specifies 802.1X critical VLANs.

guest-vlan: Specifies 802.1X guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

If you enable 802.1X unauthenticated user aging, you can set a user aging timer for Auth-Fail, critical, or guest VLANs. The user aging timer for a type of 802.1X VLAN determines how long a user can stay in that type of VLAN.

For more information about how user aging operates, see the usage guidelines on the **dot1x unauthenticated-user aging enable** command.

For a user aging timer to take effect, do not set it to a multiple of the username request timeout timer (the **dot1x timer tx-period** command).

A user aging timer change takes effect immediately.

Examples

Set the user aging timer to 150 seconds for 802.1X critical VLANs.

```
<Sysname> system-view
[Sysname] dot1x timer user-aging critical-vlan 150
```

Related commands

display dot1x

dot1x unauthenticated-user aging enable

New feature: Configuring MAC authentication unauthenticated user aging

Configuring user aging for unauthenticated MAC authentication users

About user aging for unauthenticated MAC authentication users

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Restrictions and guidelines

As a best practice, use this feature on a port only if you want to have its unauthenticated users to be authenticated and come online on a different port.

Procedure

1. Enter system view.

   system-view

2. Set the user aging timer for a type of MAC authentication VLAN.

   mac-authentication timer user-aging { **critical-vlan** | **guest-vlan** } *aging-time-value*

   By default, the user aging timer is 1000 seconds for all applicable types of MAC authentication VLANs.

3. Enter interface view.

   interface *interface-type interface-number*

4. Enable user aging for unauthenticated MAC authentication users.

   mac-authentication unauthenticated-user aging enable

   By default, user aging is enabled for unauthenticated MAC authentication users.

Command reference

mac-authentication unauthenticated-user aging enable

Use **mac-authentication unauthenticated-user aging enable** to enable user aging for unauthenticated MAC authentication users.

Use **undo mac-authentication unauthenticated-user aging enable** to disable user aging for unauthenticated MAC authentication users.

Syntax

mac-authentication unauthenticated-user aging enable

undo mac-authentication unauthenticated-user aging enable

Default

User aging is enabled for unauthenticated MAC authentication users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Examples

Disable user aging for unauthenticated MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-authentication unauthenticated-user aging enable
```

Related commands

mac-authentication timer

mac-authentication timer user-aging

Use **mac-authentication timer user-aging** to set the user aging timer for a type of MAC authentication VLAN.

Use **undo mac-authentication timer user-aging** to restore the default setting of the user aging timer for a type of MAC authentication VLAN.

Syntax

mac-authentication timer user-aging { **critical-vlan** | **guest-vlan** } *aging-time-value*

undo mac-authentication timer user-aging { **critical-vlan** | **guest-vlan** }

Default

The user aging timer is 1000 seconds for all applicable types of MAC authentication VLANs.

Views

System view

Predefined user roles

network-admin

Parameters

user-aging: Sets the user aging timer for a type of MAC authentication VLAN.

critical-vlan: Specifies MAC authentication critical VLANs.

guest-vlan: Specifies MAC authentication guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

Usage guidelines

If you enable user aging for unthenticated MAC authentication user, you can set a user aging timer for MAC authentication critical or guest VLANs. The user aging timer for a type of MAC authentication VLAN determines how long a user can stay in that type of VLAN.

For more information about how user aging operates, see the usage guidelines for the **mac-authentication unauthenticated-user aging enable** command.

Do not set the user aging timer for users in MAC authentication guest VLANs to a multiple of the authentication interval for them. If you do so, the aging timer will not take effect. The authentication interval for MAC authentication users in a guest VLAN is configurable with the **mac-authentication guest-vlan auth-period** command.

A user aging timer change takes effect immediately.

Examples

Set the user aging timer to 150 seconds for MAC authentication critical VLANs.

```
<Sysname> system-view
[Sysname] mac-authentication timer user-aging critical-vlan 150
```

Related commands

display mac-authentication

mac-authentication unauthenticated-user aging enable

New feature: VLAN check bypass for the port security MAC move feature

Enabling VLAN check bypass for the port security MAC move feature

About VLAN check bypass

VLAN check bypass enables a port to ignore the VLAN information in the packets that trigger 802.1X or MAC reauthentication for MAC move users.

The port from which the user moves is called the source port and the port to which the user moves is called the destination port.

On the destination port, an 802.1X or MAC authentication user will be reauthenticated in the VLAN authorized on the source port if the source port is enabled with MAC-based VLAN. If that VLAN is not permitted to pass through on the destination port, reauthentication will fail. To avoid this situation, enable VLAN check bypass on the destination port.

Restrictions and guidelines

When you configure VLAN check bypass for users moving between ports, follow these guidelines:

- To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
- If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags. For more information, see 802.1X configuration in *Security Configuration Guide*.

Prerequisites

For VLAN check bypass to take effect, you must enable port security MAC move.

Procedure

1. Enter system view.

system-view

2. Enable VLAN check bypass for users moving between ports.
   a. Enter interface view.
      interface *interface-type interface-number*
   b. Enable VLAN check bypass for users moving to the port from other ports.
      port-security mac-move bypass-vlan-check
      By default, the VLAN check bypass feature is disabled for users moving to a port from other ports.

Command reference

port-security mac-move bypass-vlan-check

Use **port-security mac-move bypass-vlan-check** to enable VLAN check bypass for users moving to a port from other ports.

Use **undo port-security mac-move bypass-vlan-check** to disable VLAN check bypass for users moving to a port from other ports.

Syntax

port-security mac-move bypass-vlan-check

undo port-security mac-move bypass-vlan-check

Default

VLAN check bypass is disabled for users moving to a port from other ports. When reauthenticating a user that has moved to the port, the device examines whether the VLAN to which the user belongs is permitted by the port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

VLAN check bypass skips checking VLAN information in the packets that trigger 802.1X or MAC reauthentication for users moving to the port from other ports.

On the destination port, an 802.1X or MAC authentication user will be reauthenticated in the VLAN authorized on the source port if the source port is enabled with MAC-based VLAN. If that VLAN is not permitted to pass through on the destination port, reauthentication will fail. To avoid this situation, enable VLAN check bypass on the destination port.

When you configure VLAN check bypass, follow these guidelines:

- To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
- If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags.

Examples

Enable VLAN check bypass for users moving to GigabitEthernet 1/0/1 from other ports.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-move bypass-vlan-check
```

Related commands

display port-security

dot1x eapol untag

port-security mac-move permit

New feature: Strict intrusion protection

Configuring strict intrusion protection

About strict intrusion protection

Strict intrusion protection allows the device to permanently or temporarily shut down a port if the port receives a frame that meets the following requirements: The source MAC address of the frame has been added to the secure MAC address table on another port in the same VLAN.

Restrictions and guidelines

Strict intrusion protection takes effect only when the intrusion protection action is **disableport** or **disableport-temporarily**. When strict intrusion protection is enabled on a port, you cannot change the intrusion protection action to **blockmac** on that port. To change the intrusion protection action to **blockmac**, you must first disable strict intrusion protection on that port.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Enable strict intrusion protection.

   port-security strict-intrusion-protection enable

   By default, strict intrusion protection is disabled.

Command reference

port-security strict-intrusion-protection enable

Use **port-security strict-intrusion-protection enable** to enable strict intrusion protection.

Use **undo port-security strict-intrusion-protection enable** to disable strict intrusion protection.

Syntax

port-security strict-intrusion-protection enable

undo port-security strict-intrusion-protection enable

Default

Strict intrusion protection is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Strict intrusion protection allows the device to permanently or temporarily shut down a port if the port receives a frame that meets the following requirements: The source MAC address of the frame has been added to the secure MAC address table on another port in the same VLAN.

Strict intrusion protection takes effect only when the intrusion protection action is **disableport** or **disableport-temporarily**.

Examples

Enable strict intrusion protection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security strict-intrusion-protection enable
```

Related commands

port-security intrusion-mode

port-security port-mode

New feature: Specifying the source IP address for outgoing SCP packets

Specifying the source IP address for outgoing SCP packets

About specifying the source IP address for outgoing SCP packets

After you specify the source IP address for outgoing SCP packets on an SCP client, the client uses the specified IP address to communicate with the SCP server.

Restrictions and guidelines

As a best practice, specify the IP address of a loopback interface as the source address of outgoing SCP packets for the following purposes:

- Ensuring the communication between the SCP client and the SCP server.
- Improving the manageability of SCP clients in authentication service.

Procedure

1. Enter system view.

   system-view

2. Specify the source address for outgoing SCP packets.

   IPv4:

   scp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

   By default, an SCP client uses the primary IPv4 address of the output interface in the matching route as the source address of the outgoing SCP packets.

   IPv6:

   scp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

By default, an SCP client automatically selects an IPv6 address as the source address of the outgoing packets in compliance with RFC 3484.

Command reference

scp client ipv6 source

Use **scp client ipv6 source** to configure the source IPv6 address for SCP packets that are sent by the SCP client.

Use **undo scp client ipv6 source** to restore the default.

Syntax

scp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo scp client ipv6 source

Default

The source IPv6 address for outgoing SCP packets is not configured. The SCP client automatically selects an IPv6 address for outgoing SCP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client selects the interface's address that most specifically matches the destination address of outgoing SCP packets as the source address of the SCP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SCP connections. The source IPv6 address specified in the **scp ipv6** command takes effect only on the current IPv6 SCP connection. If you specify the source IPv6 address in both this command and the **scp ipv6** command, the source IPv6 address specified in the **scp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client ipv6 source ipv6 2:2::2:2
```

Related commands

display scp client source

scp client source

Use **scp client source** to configure the source IPv4 address for SCP packets that are sent by the SCP client.

Use **undo scp client source** to restore the default.

Syntax

scp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo scp client source

Default

The source IPv4 address for outgoing SCP packets is not configured. The SCP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address for outgoing SCP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client uses the primary IPv4 address of the interface as the source address of outgoing SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SCP connections. The source IPv4 address specified in the **scp** command takes effect only on the current SCP connection. If you specify the source IPv4 address in both this command and the **scp** command, the source IPv4 address specified in the **scp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client source ip 192.168.0.1
```

Related commands

display scp client source

New feature: gRPC

About gRPC

gRPC is an open source remote procedure call (RPC) system initially developed at Google. It uses HTTP 2.0 for transport and provides network device configuration and management methods that support multiple programming languages.

gRPC protocol stack layers

Table 6 describes the gRPC protocol stack layers.

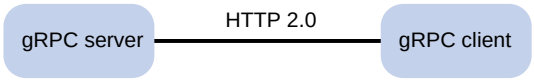
Table 6 gRPC protocol stack layers

Layer	Description
Content layer	Defines the data of the service module. Two peers must notify each other of the data models that they are using.
Protocol buffer encoding layer	Encodes data by using the protocol buffer code format.
gRPC layer	Defines the protocol interaction format for remote procedure calls.
HTTP 2.0 layer	Carries gRPC.
TCP layer	Provides connection-oriented reliable data links.

Network architecture

As shown in Figure 2, the gRPC network uses the client/server model. It uses HTTP 2.0 for packet transport.

Figure 2 gRPC network architecture



The gRPC network uses the following mechanism:

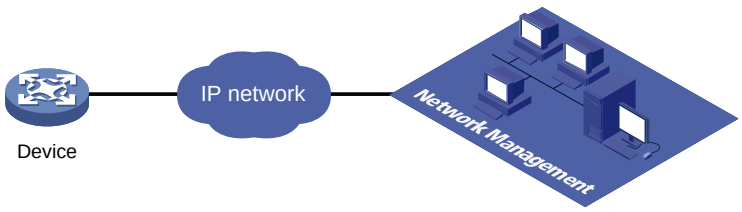
2. The gRPC server listens to connection requests from clients at the gRPC service port.
3. A user runs the gRPC client application to log in to the gRPC server, and uses methods provided in the .proto file to send requests.
4. The gRPC server responds to requests from the gRPC client.

The device can act as the gRPC server or client.

Telemetry technology based on gRPC

Telemetry is a remote data collection technology for monitoring device performance and operating status. HPE telemetry technology uses gRPC to push data from the device to the collectors on the NMSs. As shown in Figure 3, after a gRPC connection is established between the device and NMSs, the NMSs can subscribe to data of modules on the device.

Figure 3 Telemetry technology based on gRPC



Telemetry modes

The device supports the following telemetry modes:

- **Dial-in mode**—The device acts as a gRPC server and the collectors act as gRPC clients. A collector initiates a gRPC connection to the device to subscribe to device data.

  Dial-in mode applies to small networks where collectors need to deploy configurations to devices.

- **Dial-out mode**—The device acts as a gRPC client and the collectors act as gRPC servers. The device initiates a gRPC connection to the collectors and pushes subscribed device data to the collectors.

  Dial-out mode applies to larger networks where devices need to push device data to collectors.

Protocols

RFC 7540, *Hypertext Transfer Protocol version 2 (HTTP/2)*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

gRPC is not supported in FIPS mode.

Configuring the gRPC dial-in mode

gRPC dial-in mode configuration tasks at a glance

To configure the gRPC dial-in mode, perform the following tasks:

1. Configuring the gRPC service
2. Configuring a gRPC user

Configuring the gRPC service

Restrictions and guidelines

If the gRPC service fails to be enabled, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again. For more information about the **display tcp** and **display ipv6 tcp** commands, see *Layer 3—IP Services Command Reference*.

Procedure

1. Enter system view.

   system-view
2. (Optional.) Set the gRPC service port number.

   grpc port *port-number*

   By default, the gRPC service port number is 50051.
3. Enable the gRPC service.

   grpc enable

   By default, the gRPC service is disabled.
4. (Optional.) Set the gRPC session idle timeout timer.

   grpc idle-timeout *minutes*

   By default, the gRPC session idle timeout timer is 5 minutes.

Configuring a gRPC user

About gRPC users

For gRPC clients to establish gRPC sessions with the device, you must configure local users for the gRPC clients.

Procedure

1. Enter system view.

   system-view
2. Add a local user with the device management right.

   local-user *user-name* [**class manage**]
3. Configure a password for the user.

   password [{ **hash** | **simple** } *password*]

   By default, no password is configured for a local user. A non-password-protected user can pass authentication after providing the correct username and passing attribute checks.
4. Assign user role network-admin to the user.

   authorization-attribute user-role *user-role*

   By default, a local user is assigned the network-operator role.
5. Authorize the user to use the HTTPS service.

   service-type https

   By default, no service types are authorized to a local user.

For more information about the **local-user**, **password**, **authorization-attribute**, and **service-type** commands, see AAA configuration in *Security Command Reference*.

Configuring the gRPC dial-out mode

gRPC dial-out mode configuration tasks at a glance

To configure the gRPC dial-out mode, perform the following tasks:

1. Enabling the gRPC service
2. Configuring sensors
3. Configuring collectors
4. Configuring a subscription

Enabling the gRPC service

1. Enter system view.

   system-view
2. Enable the gRPC service.

   grpc enable

   By default, the gRPC service is disabled.

Configuring sensors

About sensors

The device uses sensors to sample data. A sensor path indicates a data source.

Supported data sampling types include:

- **Event-triggered sampling**—Sensors in a sensor group sample data when certain events occur. For sensor paths of this data sampling type, see *NETCONF XML API Event Reference* for the module.
- **Periodic sampling**—Sensors in a sensor group sample data at intervals. For sensor paths of this data sampling type, see the NETCONF XML API references for the module except for *NETCONF XML API Event Reference*.

Procedure

1. Enter system view.

   system-view
2. Enter telemetry view.

   telemetry
3. Create a sensor group and enter sensor group view.

   sensor-group *group-name*
4. Specify a sensor path.

   sensor path *path*

   To specify multiple sensor paths, execute this command multiple times.

Configuring collectors

About collectors

Collectors are used to receive sampled data from network devices. For the device to communicate with collectors, you must create a destination group and add collectors to the destination group.

Restrictions and guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Procedure

1. Enter system view.

   system-view
2. Enter telemetry view.

   telemetry
3. Create a destination group and enter destination group view.

   destination-group *group-name*
4. Specify a collector.

   IPv4:

   ipv4-address *ipv4-address* [**port** *port-number*]

   IPv6:

   ipv6-address *ipv6-address* [**port** *port-number*]

   To specify multiple collectors, execute this command multiple times. One collector must have a different address, port.

Configuring a subscription

About configuring a subscription

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

Procedure

1. Enter system view.

   system-view

2. Enter telemetry view.

   telemetry

3. Create a subscription and enter subscription view.

   subscription *subscription-name*

4. (Optional.) Specify the source IP address for packets sent to collectors.

   source-address { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

   By default, the device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

   Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

5. Specify a sensor group.

   sensor-group *group-name* [**sample-interval** *interval*]

   Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths.

   - If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
   - If you do not specify the option for periodic sensor paths, the device does not sample or push data.

6. Specify a destination group.

   destination-group *group-name*

Display and maintenance commands for gRPC

Execute **display** commands in any view.

Task	Command
Display gRPC information in dial-in mode.	**display grpc**

gRPC configuration examples

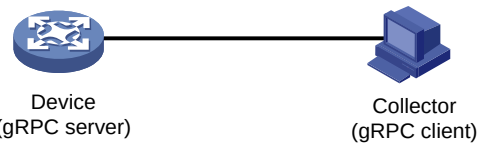
These configuration examples describe only CLI configuration tasks on the device. The collectors need to run an extra application.

Example: Configuring the gRPC dial-in mode

Network configuration

As shown in Figure 4, configure the gRPC dial-in mode on the device so the device acts as the gRPC server and the gRPC client can subscribe to LLDP events on the device.

Figure 4 Network diagram



Procedure

1. Assign IP addresses to interfaces on the gRPC server and client and configure routes. Make sure the server and client can reach each other.
2. Configure the device as the gRPC server:

   # Enable the gRPC service.

   ```
   <Device> system-view
   [Device] grpc enable
   ```

   # Create a local user named **test**. Set the password to **test**, and assign user role network-admin and the HTTPS service to the user.

   ```
   [Device] local-user test
   [Device-luser-manage-test] password simple test
   [Device-luser-manage-test] authorization-attribute user-role network-admin
   [Device-luser-manage-test] service-type https
   [Device-luser-manage-test] quit
   ```
3. Configure the gRPC client.
   a. Prepare a PC and install the gRPC environment on the PC. For more information, see the user guide for the gRPC environment.
   b. Obtain the HPE proto definition file and uses the protocol buffer compiler to generate code of a specific language, for example, Java, Python, C/C++, or Go.
   c. Create a client application to call the generated code.
   d. Start the application to log in to the gRPC server.

Verifying the configuration

When an LLDP event occurs on the gRPC server, verify that the gRPC client receives the event.

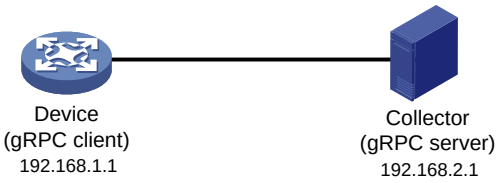
Example: Configuring the gRPC dial-out mode

Network configuration

As shown in Figure 5, the device is connected to a collector. The collector uses port 50050.

Configure gRPC dial-out mode on the device so the device pushes the device capability information of its interface module to the collector at 10-second intervals.

Figure 5 Network diagram



Procedure

Configure IP addresses as required so the device and the collector can reach each other. (Details not shown.)

Enable the gRPC service.

```
<Device> system-view
[Device] grpc enable
```

Create a sensor group named **test**, and add sensor path **ifmgr/devicecapabilities/**.

```
[Device] telemetry
[Device-telemetry] sensor-group test
[Device-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
[Device-telemetry-sensor-group-test] quit
```

Create a destination group named **collector1**. Specify a collector that uses IPv4 address 192.168.2.1 and port number 50050.

```
[Device-telemetry] destination-group collector1
[Device-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Device-telemetry-destination-group-collector1] quit
```

Configure a subscription named **A** to bind sensor group **test** with destination group **collector1**. Set the sampling interval to 10 seconds.

```
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
[Device-telemetry-subscription-A] destination-group collector1
[Device-telemetry-subscription-A] quit
```

Verifying the configuration

Verify that the collector receives the device capability information of the interface module from the device at 10-second intervals. (Details not shown.)

gRPC dial-in mode commands

display grpc

Use **display grpc** to display gRPC dial-in mode information.

Syntax

display grpc

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display gRPC dial-in mode information.

```
<Sysname> display grpc
gRPC status : enabled.
gRPC port : 50051
gRPC idle-timeout : 3 minutes
Session count: 1.
  Session ID: 1
    User name: test
    Login time:2018-01-05 06:46:43 Idle time : 2 mins 56 s
    Client IP address : 169.254.100.170:40810
    Received RPCs        : 0         Received error RPCs : 0
    Received subscription: 0         Output notifications: 0
```

Table 7 Command output

Field	Description
gRPC status	Status of the gRPC service: • **enabled**—The gRPC service is enabled. • **disabled**—The gRPC service is disabled.
gRPC idle-timeout	Setting for the gRPC session idle timeout timer.
Session count	Number of gRPC sessions.
Idle time	Duration in which the session idle timeout timer will expire. If the value of this field is 0, gRPC sessions will never be timed out.
Received error RPCs	Number of received erroneous gRPC requests.
Received subscription	Number of received gRPC subscription requests.

grpc enable

Use **grpc enable** to enable the gRPC service.

Use **undo grpc enable** to disable the gRPC service.

Syntax

grpc enable

undo grpc enable

Default

The gRPC service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If this command fails, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again.

Examples

Enable the gRPC service.

```
<Sysname> system
[Sysname] grpc enable
```

Related commands

display ipv6 tcp (*Layer 3—IP Services Command Reference*)

display tcp (*Layer 3—IP Services Command Reference*)

grpc port

grpc idle-timeout

Use **grpc idle-timeout** to set the gRPC session idle timeout timer.

Use **undo grpc idle-timeout** to restore the default.

Syntax

grpc idle-timeout *minutes*

undo grpc idle-timeout

Default

The gRPC session idle timeout timer is 5 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the gRPC session idle timeout timer in minutes, in the range of 0 to 30. To disable gRPC sessions from being timed out, set it to 0.

Usage guidelines

If no gRPC packet exchanges occur on the session between a gRPC and the server before the idle timeout timer expires, the device closes the session.

Examples

Set the gRPC session idle timeout timer to 6 minutes.

```
<Sysname> system
[Sysname] grpc idle-timeout 6
```

grpc port

Use **grpc port** to specify the gRPC service port number.

Use **undo grpc port** to restore the default.

Syntax

grpc port *port-number*

undo grpc port

Default

The gRPC service port number is 50051.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the gRPC service port number, in the range of 1 to 65535.

Usage guidelines

You can configure this command only when the gRPC service is disabled.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the gRPC service port number to 50052.

```
<Sysname> system
[Sysname] grpc port 50052
```

Related commands

grpc enable

gRPC dial-out mode commands

destination-group (subscription view)

Use **destination-group** to specify a destination group for a subscription.

Use **undo destination-group** to remove a destination group from a subscription.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

A subscription does not have a destination group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a destination group by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

The specified destination group must have been created by using the **destination-group** command in telemetry view.

You can specify a maximum of five destination groups for a subscription.

Examples

Specify destination group **collector1** for subscription **A**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] destination-group collector1
```

Related commands

destination-group (telemetry view)

destination-group (telemetry view)

Use **destination-group** to create a destination group and enter its view, or enter the view of an existing destination group.

Use **undo destination-group** to delete a destination group.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

No destination groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the destination group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Examples

Create a destination group named **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1]
```

ipv4-address

Use **ipv4-address** to add an IPv4 collector to a destination group.

Use **undo ipv4-address** to remove an IPv4 collector from a destination group.

Syntax

ipv4-address *ipv4-address* [**port** *port-number*]

undo ipv4-address *ipv4-address* [**port** *port-number*]

Default

A destination group does not have IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address or port than the other collectors.

You can specify a maximum of five collectors for a destination group.

Examples

Add a collector that uses IPv4 address 192.168.21.21 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.21.21
```

Related commands

destination-group (telemetry view)

ipv6-address

Use **ipv6-address** to add an IPv6 collector to a destination group.

Use **undo ipv6-address** to remove an IPv6 collector from a destination group.

Syntax

ipv6-address *ipv6-address* [**port** *port-number*]

undo ipv6-address *ipv6-address* [**port** *port-number*]

Default

A destination group does not have IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address or port than the other collectors.

You can specify a maximum of five collectors for a destination group.

Examples

Add a collector that uses IPv6 address 1: : 1 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6-address 1: : 1
```

Related commands

destination-group (telemetry view)

sensor path

Use **sensor path** to configure a sensor path.

Use **undo sensor path** to delete a sensor path.

Syntax

sensor path *path*

undo sensor path *path*

Default

No sensor paths exist.

Views

Sensor group view

Predefined user roles

network-admin

Parameters

path: Specifies a data path. For information about the available paths, enter a question mark (?) in the position of this argument.

Usage guidelines

To configure multiple sensor paths, execute this command multiple times.

The device supports a maximum of 128 sensor paths.

If the device does not support the specified sensor path, the command displays an error message.

Examples

Configure sensor path **ifmgr/devicecapabilities/** for sensor group **test**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
```

Related commands

sensor-group (telemetry view)

sensor-group (subscription view)

Use **sensor-group** to specify a sensor group for a subscription.

Use **undo sensor-group** to remove a sensor group from a subscription.

Syntax

sensor-group *group-name* [**sample-interval** *interval*]

undo sensor-group *group-name*

Default

A subscription does not have a sensor group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

group-name: Specifies a sensor group by its name, a case-sensitive string of 1 to 31 characters.

sample-interval *interval*: Specifies the data sampling interval in seconds. The value range is 1 to 86400.

Usage guidelines

Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths.

- If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
- If you do not specify the option for periodic sensor paths, the device does not sample or push data.

The specified sensor group must have been created by using the **sensor-group** command in telemetry view.

Examples

Specify sensor group **test** for subscription **A**. Set the data sampling interval to 10 seconds.

```
<Sysname> system-view
[Sysname] telemetry
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
```

Related commands

sensor path

sensor-group (telemetry view)

sensor-group (telemetry view)

Use **sensor-group** to create a sensor group and enter its view, or enter the view of an existing sensor group.

Use **undo sensor-group** to delete a sensor group.

Syntax

sensor-group *group-name*

undo sensor-group *group-name*

Default

No sensor groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the sensor group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 32 sensor groups.

Examples

Create a sensor group named **test**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test]
```

source-address

Use **source-address** to specify the source IP address for packets sent to collectors.

Use **undo source-address** to restore the default.

Syntax

source-address { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo source-address

Default

The device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

Views

Subscription view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. In the current software version, you must specify a loopback interface. The device will use the interface's primary IPv4 address as the source address. If the interface does not have a primary IPv4 address, the device uses the primary IPv4 address of the output interface for the route to the collectors.

ipv6 *ipv6-address*: Specifies an IPv6 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

Examples

Specify the source IPv4 address of 169.254.1.1 for packets sent to collectors.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] source-address 169.254.1.1
```

subscription

Use **subscription** to create a subscription and enter its view, or enter the view of an existing subscription.

Use **undo sensor-group** to delete a subscription.

Syntax

subscription *subscription-name*

undo subscription *subscription-name*

Default

No subscription groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

subscription-name: Specifies the subscription name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 10 subscriptions.

Examples

Configure a subscription named **A**.

```
<Sysname> system-view
```

```
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A]
```

Related commands

destination-group (subscription view)

sensor-group (subscription view)

telemetry

Use **telemetry** to enter telemetry view.

Syntax

telemetry

Views

System view

Predefined user roles

network-admin

Usage guidelines

In telemetry view, you can configure telemetry parameters.

Examples

Enter telemetry view.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry]
```

Modified feature: Specifying the HTTPS redirect listening port number

Feature change description

The default setting for the HTTPS redirect listening port number was changed.

Command changes

Modified command: http-redirect https-port

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

Views

System view

Change description

Before modification: By default, the HTTPS redirect listening port number is not specified.

After modification: By default, the HTTPS redirect listening port number is 6654.

Modified feature: Specifying startup images

Feature change description

In addition to boot, system, feature images, you can specify patch images when you specify startup images.

Command changes

Modified command: boot-loader file

Old syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

New syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Change description

Before modification: The command does not support the **patch** *filename*&<1-16> option.

After modification: The command supports the **patch** *filename*&<1-16> option.

Modified feature: Automatic configuration

Feature change description

Before modification: To verify automatization configuration, you must examine the configuration file.

After modification: You can verify automatization configuration also by observing the system status LED. After the device starts up correctly, its system status LED turns steady green. After the device starts automatic configuration, its system status LED flashes green. After the device finishes automatic configuration, its system status LED turns steady green again.

Command changes

None.

Modified feature: Displaying ARP snooping entries

Feature change description

The syntax of the command to display ARP snooping entries was changed.

Command changes

Modified command: display arp snooping

Old syntax

display arp snooping [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping ip *ip-address* [**slot** *slot-number*]

New syntax

display arp snooping vlan [*vlan-id*] [**slot** *slot-number*] [**count**]

display arp snooping vlan ip *ip-address* [**slot** *slot-number*]

Views

Any view

Change description

Before modification: The **vlan** keyword is optional.

After modification: The **vlan** keyword is required.

Modified feature: Clearing ARP snooping entries

Feature change description

The syntax of the command to clear ARP snooping entries was changed.

Command changes

Modified command: reset arp snooping

Old syntax

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

New syntax

reset arp snooping vlan [*vlan-id*]

reset arp snooping vlan ip *ip-address*

Views

Any view

Change description

Before modification: The **vlan** keyword is optional.

After modification: The **vlan** keyword is required.

Modified feature: Setting the DHCP server response timeout time for DHCP server switchover

Feature change description

In this release, the value range for DHCP server response timeout time for DHCP server switchover was changed to 1 to 65535 seconds.

Command changes

Modified command: dhcp relay dhcp-server timeout

Syntax

dhcp relay dhcp-server timeout *time*

Default

The DHCP server response timeout time is 30 seconds.

Views

Interface view

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Change description

Before modification: The value range for the *time* argument is 30 to 65535 seconds.

After modification: The value range for the *time* argument is 1 to 65535 seconds.

Modified command: dhcp-server timeout

Syntax

dhcp-server timeout *time*

Default

The DHCP server response timeout time is 30 seconds.

Views

DHCP address pool view

Parameters

time: Specifies the DHCP server response timeout time in the range of 1 to 65535 seconds.

Change description

Before modification: The value range for the *time* argument is 30 to 65535 seconds.

After modification: The value range for the *time* argument is 1 to 65535 seconds.

Modified feature: Automatic configuration

Feature change description

Before modification: The device supports automatic configuration only on IPv4 networks.

After modification: The device supports automatic configuration on both IPv4 and IPv6 networks.

Command changes

None.

Modified feature: Physical type of a combo interface

Feature change description

In this version and later, the **auto** keyword is added to the **combo enable** command. This keyword configures a combo interface to automatically recognize the media inserted and activate the corresponding physical port.

Command changes

Modified command: combo enable

Old syntax

combo enable { **copper** | **fiber** }

New syntax

combo enable { auto | copper | fiber }

Views

Ethernet interface view

Parameters

auto: Specifies the combo interface to autonegotiate its physical type.

Usage guidelines

When a combo interface acts as an IRF physical interface, you must manually configure the physical type of the combo interface as **copper** or **fiber**.

A combo interface in **auto** mode does not support the **duplex half**, **speed 10**, or **speed 100** command.

Change description

Before modification:

By default, the copper combo port is activated. You can specify the **copper** or **fiber** keyword to activate the copper or fiber combo port as needed.

After modification:

By default, a combo interface autonegotiates its physical type. When a combo autonegotiates its physical type, the actual physical type depends on the connected media:

- When the copper combo port is not connected to a twisted-pair cable and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
- When the copper combo port is connected to a twisted-pair cable and is up:
  a. If you install a transceiver module in the fiber combo port, the copper combo port is still activated before the device is rebooted.
  b. After the device is rebooted, the fiber combo port is activated.
- When the copper combo port is connected to a twisted-pair cable and is down and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
- When the fiber combo port has a transceiver module installed, the fiber combo port is activated even if you connect a twisted-pair cable to the copper combo port.

If you need to specify the physical type of a physical interface according to the network requirements, you can specify the **copper** or **fiber** keyword to activate the copper or fiber combo port.

Modified feature: Physical state change suppression

Feature change description

In this version and later, the syntax for configuring physical state change suppression on Ethernet interfaces and aggregate interfaces is modified.

Command changes

Modified command: link-delay

Old syntax

link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

undo link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

New syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Parameters

down: Suppresses link-down events.

up: Suppresses link-up events.

msec: Enables the physical state change suppression interval to be accurate to milliseconds. If you do not specify this keyword, the suppression interval is accurate to seconds.

delay-time: Sets the physical state change suppression interval. A value of 0 means that physical state changes are immediately reported to the CPU and are not suppressed.

- If you do not specify the **msec** keyword, the physical state change suppression interval is in seconds and the value range is 0 to 30.
- If you specify the **msec** keyword, the value range is 0 to 10000 milliseconds, and the value must be a multiple of 100.

Change description

Before modification:

- If the **mode** keyword is not specified, the link-down events are suppressed.
- If the **mode up** keyword combination is specified, the link-up events are suppressed.
- If the **mode updown** keyword combination is specified, both link-down and link-up events are suppressed.
- If the suppression interval configured in the command without the **mode** keyword specified is the same as the suppression interval configured in the command with the **mode up** keyword combination specified on an interface, the two commands are automatically merged into the command with the **mode updown** keyword combination specified in the configuration file of the interface.

After modification:

- If the **down** keyword is not specified, the link-down events are suppressed.
- If the **up** keyword is specified, the link-up events are suppressed.
- You can set different link state change suppression intervals for link-down events and link-up events.

Modified feature: MAC-to-VLAN entries

Feature change description

In this version and later, the keyword for configuring 802.1p priorities in MAC-to-VLAN entries is modified to **dot1p**.

Command changes

Modified command: mac-vlan mac-address

Old syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]

New syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]

Views

System view

Change description

Before modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is **dot1q**.

After modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is **dot1p**.

Modified command: display mac-vlan

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }

Views

Any view

Old command output

Display all MAC-to-VLAN entries.

```
<Sysname> display mac-vlan all
The following MAC VLAN entries exist:
State: S - Static, D - Dynamic
MAC address        Mask               VLAN ID   Dot1q      State
0008-0001-0000     ffff-ff00-0000     5         3          S
0002-0001-0000     ffff-ffff-ffff     5         3          S&D
Total MAC VLAN entries count: 2
```

New command output

Display all MAC-to-VLAN entries.

```
<Sysname> display mac-vlan all
The following MAC VLAN entries exist:
State: S - Static, D - Dynamic
MAC address        Mask               VLAN ID   Dot1p      State
0008-0001-0000     ffff-ff00-0000     5         3          S
0002-0001-0000     ffff-ffff-ffff     5         3          S&D
Total MAC VLAN entries count: 2
```

Change description

Before modification: The field for displaying the 802.1p priority of a VLAN was Dot1q.

After modification: The field for displaying the 802.1p priority of a VLAN was Dot1p.

Modified feature: Displaying the loop detection configuration and status

Feature change description

Information about shutdown interfaces was added to the output from the **display loopback-detection** command.

Command changes

Modified command: display loopback-detection

Syntax

display loopback-detection

Views

Any view

Change description

Before modification: If the loop protection action is set to shutdown, this command does not display the interfaces shut down by loop detection.

Display the loop detection configuration and status.

```
<Sysname> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
No loopback is detected.
```

After modification: If the loop protection action is set to shutdown, this command displays the interfaces shut down by loop detection.

Display the loop detection configuration and status.

```
<Sysname> display loopback-detection
Loop detection is enabled.
Loop detection interval is 30 second(s).
Loop is detected on following interfaces:
 Interface                Action mode     VLANs
 GigabitEthernet1/0/1     Shutdown        10
```

Modified feature: Setting the 802.1p priority for IGMP messages

Feature change description

The default 802.1p priority of IGMP messages was changed to 6.

Command changes

Modified command: dot1p-priority

Syntax

dot1p-priority *priority*

undo dot1p-priority

Views

IGMP-snooping view

Change description

Before modification: By default, the 802.1p priority of IGMP messages is not configured. For IGMP messages generated by the device, the 802.1p priority is 0. For IGMP messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of IGMP messages is 6.

Modified command: igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

Views

VLAN view

Change description

Before modification: By default, the 802.1p priority of IGMP messages is not configured. For IGMP messages generated by the device, the 802.1p priority is 0. For IGMP messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of IGMP messages is 6.

Modified feature: Setting the 802.1p priority for MLD messages

Feature change description

The default 802.1p priority of MLD messages was changed to 6.

Command changes

Modified command: dot1p-priority

Syntax

dot1p-priority *priority*

undo dot1p-priority

Views

MLD-snooping view

Change description

Before modification: By default, the 802.1p priority of MLD messages is not configured. For MLD messages generated by the device, the 802.1p priority is 0. For MLD messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of MLD messages is 6.

Modified command: mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

Views

VLAN view

Change description

Before modification: By default, the 802.1p priority of MLD messages is not configured. For MLD messages generated by the device, the 802.1p priority is 0. For MLD messages forwarded by the device, the 802.1p priority remains unchanged.

After modification: By default, the 802.1p priority of MLD messages is 6.

Modified feature: Displaying IPv4SG bindings

Feature change description

The **arp-snooping** keyword was changed to the **arp-snooping-vlan** keyword in the command syntax.

Command changes

Modified command: display ip source binding

Old syntax

display ip source binding [**static** | [**arp-snooping** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

New syntax

display ip source binding [**static** | [**arp-snooping-vlan** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Change description

The **arp-snooping-vlan** keyword replaces the **arp-snooping** keyword in the command to specify dynamic IPv4SG bindings generated based on ARP snooping.

Modified feature: Displaying IPv6SG bindings

Feature change description

The **nd-snooping** keyword was changed to the **nd-snooping-vlan** keyword in the command syntax.

Command changes

Modified command: display ipv6 source binding

Old syntax

display ipv6 source binding [**static** | [**dhcpv6-relay** | **dhcpv6-snooping** | **dot1x** | **nd-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

New syntax

display ipv6 source binding [**static** | [**dhcpv6-relay** | **dhcpv6-snooping** | **dot1x** | **nd-snooping-vlan**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Change description

The **nd-snooping-vlan** keyword replaces the **nd-snooping** keyword in the command to specify dynamic IPv4SG bindings generated based on ND snooping.

Modified feature: Displaying the MFF configuration for a VLAN

Feature change description

In this release, the **display mac-forced-forwarding vlan** command does not support displaying the MFF operating mode.

Command changes

Modified command: display mac-forced-forwarding vlan

Syntax

display mac-forced-forwarding vlan *vlan-id*

Views

Any view

Examples

Before modification:

Display the MFF configuration for VLAN 2.

```
<Sysname> display mac-forced-forwarding vlan 2
VLAN 2
Mode: Manual/Single
Gateway:
------------------------------------------------------------------------------
192.168.1.42         000f-e200-8046
Server:
------------------------------------------------------------------------------
192.168.1.48         192.168.1.49
```

Table 8 Command output

Field	Description
VLAN 2	ID of the VLAN to which the gateways belong.
Mode	MFF operating mode: • Manual (Manual). • Single-gateway (Single).
Gateway	IP and MAC addresses of gateways. If no address is learned, this field displays **N/A**.

Field	Description
Server	Server IP addresses.

After modification:

Display the MFF configuration for VLAN 2.

```
<Sysname> display mac-forced-forwarding vlan 2
VLAN 2
Gateway:
------------------------------------------------------------------------------
192.168.1.42         000f-e200-8046
Server:
------------------------------------------------------------------------------
192.168.1.48         192.168.1.49
```

Table 9 Command output

Field	Description
VLAN 2	ID of the VLAN to which the gateways belong.
Gateway	IP and MAC addresses of gateways. If no address is learned, this field displays **N/A**.
Server	Server IP addresses.

Change description

Before modification: The **display mac-forced-forwarding vlan** command supports displaying the **Mode** field.

After modification: The **display mac-forced-forwarding vlan** command does not support displaying the **Mode** field.

Modified feature: Associating Track with application modules

Feature change description

From this release, you cannot configure the notification delay when associating Track with application modules. Creating a track entry associated with an application module enters Track view. You can configure the delay only in Track view for notifying the application module of track entry state changes.

Command changes

Modified command: track bfd ctrl

Old syntax

track *track-entry-number* **bfd ctrl** [**interface** *interface-type interface-number*] **remote ip** *remote-ip-address* **local ip** *local-ip-address* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **bfd ctrl** [**interface** *interface-type interface-number*] **remote ip** *remote-ip-address* **local ip** *local-ip-address*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track bfd echo

Old syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip-address* **local ip** *local-ip-address*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track cfd

Old syntax

track *track-entry-number* **cfd cc service-instance** *instance-id* **mep** *mep-id* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **cfd cc service-instance** *instance-id* **mep** *mep-id*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track interface

Old syntax

track *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **interface** *interface-type interface-number*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track interface physical

Old syntax

track *track-entry-number* **interface** *interface-type interface-number* **physical** [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **interface** *interface-type interface-number* **physical**

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track interface protocol

Old syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** }

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track ip route reachability

Old syntax

track *track-entry-number* **ip route** *ip-address* { *mask-length* | *mask* } **reachability** [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **ip route** *ip-address* { *mask-length* | *mask* } **reachability**

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track lldp neighbor

Old syntax

track *track-entry-number* **lldp neighbor interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **lldp neighbor interface** *interface-type interface-number*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified command: track nqa

Old syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

New syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

Modified feature: Configuring binding attributes for local users

Feature change description

As from this version, the device supports configuring binding interfaces for device management users.

Command changes

Modified command: bind-attribute

Syntax

bind-attribute { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

Views

Local user view

Change description

Before modification: The **location interface** *interface-type interface-number* option is applicable only to LAN and portal users.

After modification: The **location interface** *interface-type interface-number* option is applicable to device management users in addition to LAN and portal users.

Modified feature: Enabling password control

Feature change description

This release supports enabling password control globally for network access users.

Command changes

Modified command: password-control enable

Old syntax

password-control enable

undo password-control enable

New syntax

password-control enable [**network-class**]

undo password-control enable [**network-class**]

Views

System view

Change description

Before modification: You can enable the password control feature globally only for device management users.

After modification: The **network-class** keyword was added. You can enable the password control feature globally for both device management users and network access users.

Modified feature: Password management after global password control is enabled

Feature change description

Managing local user passwords for device management users

Before modification:

- A password set in plaintext form is stored in ciphertext form, and a password set in hashed form is not stored.
- If a user changes its own password in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If the user changes its own password in hashed form, the system does not compare the new password with the current password or passwords in the history records.
- If a user deletes its own password, the system does not request the user to enter the current plaintext password.
- In FIPS mode, if a user with the network-admin user role changes its password, the system does not request the user to enter the current plaintext password.

After modification:

- All passwords in the history records are saved in hashed form.
- If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
- If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.
- If a user deletes its own password, the system requests the user to enter the current plaintext password.
- Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with passwords in the history records and the current password.

Managing super passwords

Before modification:

- If a super new password is set in plaintext form, the password is saved in encrypted form. If a new super password is set in hashed form, the password is not saved.
- If a super password is changed in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If a super password is changed in hashed form, the system does not compare the new password with the current password and passwords in the history records.

After modification:

- All super passwords in the history records are saved in hashed form.
- If a super password is changed in plaintext form, the new password must be different from all passwords in the history records and the current password. If a super password is changed in hashed form, the system does not compare the new password with the current one and those stored in the history password records.

Command changes

None.

Modified feature: Setting the quiet timer for RADIUS servers in a RADIUS scheme

Feature change description

The minimum value of the quiet time for RADIUS servers was changed from 1 minute to 0 minutes.

Command changes

Modified command: timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

Views

RADIUS scheme view

Change description

Before modification: The value range for the *minutes* argument is 1 to 255, in minutes.

After modification: The value range for the *minutes* argument is 0 to 255, in minutes. If you set this argument to 0, the device does not change the state of the current server for a user when the server is unreachable. It sends an authentication or accounting request of the user to the next server in active state. For an authentication or accounting request of a new user, it still tries to send the request to the current server because the current server is in active state.

Modified feature: MAC-based MAC authentication user accounts for MAC authentication

Feature change description

As from this version, the device allows you to configure a password shared by all MAC-based MAC authentication user accounts.

Command changes

Modified command: mac-authentication user-name-format

Old syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }

New syntax

mac-authentication user-name-format { **fixed** [**account** *name*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] } [**password** { **cipher** | **simple** } *string*]

Views

System view

Change description

Before modification: You cannot specify a password for MAC-based MAC authentication user accounts. The MAC address of each user is used as their password.

After modification: You can specify a password for all MAC-based MAC authentication user accounts by using the **password** { **cipher** | **simple** } *string* option. If you do not specify a password, each user uses its own MAC address as the password.

Modified feature: MAC authentication VLAN mode

Feature change description

As from this version, the port security MAC move feature determines how a port in MAC authentication single-VLAN mode handles an online user with an authorization VLAN when that user moves between VLANs.

Before modification:

In single-VLAN mode, the port does not reauthenticate an online user when traffic from that user contains a VLAN tag different than the VLAN in which the user was authenticated. The user will stay online in the authorization VLAN and cannot access any other VLANs until a logoff occurs.

After modification:

In single-VLAN mode, the port reauthenticates an online user when traffic received from that user contains a VLAN tag different from the VLAN in which the user was authenticated. The authentication process differs depending on the MAC move setting in port security, as follows:

- If MAC move is disabled in port security, the user cannot pass authentication and come online from the new VLAN until after it goes offline from the port.
- If MAC move is enabled in port security, the user can pass authentication on the new VLAN and come online without having to first go offline from the port. After the user passes authentication on the new VLAN, the original authentication session of the user is deleted from the port.

No changes were introduced to the command syntax.

NOTE:

- To enable single-VLAN mode, execute the **undo** form of the **mac-authentication host-mode multi-vlan** command.
- To enable the port security MAC move feature, use the **port-security mac-move permit** command.

Modified feature: Web authentication

Before modification: Web authentication supports only HTTP redirect. It does not support HTTPS redirect.

After modification: Web authentication supports both HTTP redirect and HTTPS redirect. To enable the device to redirect HTTPS packets in Web authentication, specify the HTTPS redirect listening port number by using the **http-redirect https-port** command in system view.

Modified feature: Port security NTK feature

Feature change description

As from this version, the device supports the ntkauto mode for the need to known (NTK) feature of port security. A port in ntkauto mode forwards only broadcast, multicast, and unicast frames with an authenticated destination MAC address, and only when the port has online users.

Command changes

Modified command: port-security ntk-mode

Old syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

New syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkauto** | **ntkonly** }

Views

Layer 2 Ethernet interface view

Change description

Before modification: The **ntkauto** keyword was not available.

After modification: The **ntkauto** keyword was added to this command.

Modified feature: Port security MAC move

Feature change description

As from this version, the port security MAC move feature takes effect on users that move between VLANs on a port in addition to users that move between ports.

Before modification: Port security MAC move setting takes effect only on users that move between ports on the device.

After modification: Port security MAC move setting also take effect on users that move between VLANs on a port.

- If this feature is disabled, authenticated users must go offline from the original VLAN first before they can be reauthenticated successfully on the new VLAN and come online.
- If this feature is enabled, authenticated users can be reauthenticated successfully on the new VLAN without having to go offline from the original VLAN. The port will remove the users from the original VLAN immediately after the users are reauthenticated successfully on the new VLAN.

No changes were introduced to the command syntax.

NOTE:

MAC authentication multi-VLAN mode has higher priority than MAC move for users moving between VLANs on a port. If MAC authentication multi-VLAN mode is enabled, these users can come online in the new VLAN without being reauthenticated. To enable MAC authentication multi-VLAN mode, use the **mac-authentication host-mode multi-vlan** command.

Modified feature: RSA key modulus length used for creating an RSA key pair

Feature change description

The value range for the key modulus length used for creating an RSA local key pair was changed.

Command changes

Modified command: public-key local create

Syntax

In non-FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

In FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

Views

System view

Change description

Before modification:

- In non-FIPS mode, the RSA key modulus length is in the range of 512 to 2048 bits. The default is 1024 bits.
- In FIPS mode, the RSA key modulus length is 2048 bits.

After modification:

- In non-FIPS mode, the RSA key modulus length is in the range of 512 to 4096 bits. The default is 1024 bits.
- In FIPS mode, the RSA key modulus length is a multiple of 256 in the range of 2048 to 4096 bits. The default is 2048 bits.

Modified feature: RSA key modulus length used for PKI certificate request

Feature change description

In PKI domain view, the value range for the RSA key modulus length used for certificate request was changed.

Command changes

Modified command: public-key rsa

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

Views

PKI domain view

Change description

Before modification:

- In non-FIPS mode, the RSA key modulus length (*key-length*) is in the range of 512 to 2048 bits. The default is 1024 bits.
- In FIPS mode, the RSA key modulus length (*key-length*) is 2048 bits.

After modification:

- In non-FIPS mode, the RSA key modulus length (*key-length*) is in the range of 512 to 4096 bits. The default is 1024 bits.
- In FIPS mode, the RSA key modulus length (*key-length*) is a multiple of 256 in the range of 2048 to 4096 bits. The default is 2048 bits.

Modified feature: SNMP notifications for IKE

Feature change description

From this version, all SNMP notifications for IKE are disabled by default.

Command changes

Modified command: snmp-agent trap enable ike

Syntax

snmp-agent trap enable ike [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **global** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal-delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *

Views

System view

Change description

Before modification: All SNMP notifications for IKE are enabled by default.

After modification: All SNMP notifications for IKE are disabled by default.

Modified feature: Configuring an SNMP notification target host

Feature change description

A DSCP value can be set for SNMP notifications sent to the target host.

Command changes

Modified command: snmp-agent target-host

Old syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

In FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

New syntax

In non-FIPS mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string*

In FIPs mode:

snmp-agent target-host inform address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

snmp-agent target-host trap address udp-domain { *ipv4-target-host* | **ipv6** *ipv6-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6-target-host* } **params securityname** *security-string*

Default

No SNMP notification target hosts exist.

Views

System view

Parameters

dscp-value: Sets the DSCP value for notifications sent to the target host, in the range of 0 to 63. The default value is 0. A greater DSCP value represents a higher priority. The DSCP value is encapsulated in the ToS field of an IP packet and affects the forwarding priority of the packet.

Change description

The **dscp** *dscp-value* option was added to the command.

Modified feature: Displaying logs buffered over the last specified period of time

Feature change description

From this release, you can display logs buffered over the last specified period of time.

Command changes

Modified command: display logbuffer

Old syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] *

New syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] * [**last-mins** *mins*]

Views

Any view

Examples

Display log buffer information and logs buffered over the last 5 minutes.

```
<Sysname> display logbuffer last-mins 5
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
```

```
Current messages: 191
%Jan  1 01:00:06:784 2011 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.1.242-User=**; Command is display current-configuration
%Jan  1 01:03:19:691 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.33.
%Jan  1 01:03:21:269 2018 Sysname SHELL/6/SHELL_CMD:
-Line=vty1-IPAddr=192.168.1.33-User=**; Command is display logbuffer last-mins 5
```

Change description

The **last-mins** *mins* option was added to the command.

last-mins *mins*: Displays logs buffered over the last specified period of time. The *mins* argument specifies a time period in the range of 1 to 43200 minutes. If you do not specify a time period, the command displays all logs in the log buffer.

Modified feature: Specifying a log host and its output parameters

Feature change description

From this release, you can specify the DSCP value in log packets sent to a log host and set the timestamp to be accurate to milliseconds for logs output to log hosts.

Command changes

Modified command: info-center loghost

Old syntax

info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]

New syntax

info-center loghost { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*]

Default

No log hosts are specified.

Views

System view

Change description

The **dscp** *dscp-value* option was added to the command.

dscp *dscp-value*: Specifies the DSCP value in log packets sent to the log host. The value range for the *dscp-value* argument is 0 to 63, and the default is 0. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority.

Modified command: info-center timestamp loghost

Old syntax

info-center timestamp loghost { **date** | **iso** [**with-timezone**] | **no-year-date** | **none** }

undo info-center timestamp loghost

New syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }

undo info-center timestamp loghost

Views

System view

Change description

The **with-milliseconds** keyword was added to the command.

with-milliseconds: Sets the timestamp to be accurate to milliseconds for logs output to log hosts in date or ISO 8601 format. The millisecond value is appended to the time information in the timestamp with a dot as the separator. If you do not specify this keyword, the timestamp in date or ISO 8601 format is accurate to seconds.

- Example of a timestamp in date format with millisecond accuracy: Dec 8 10:12:21.708 2018.
- Example of a timestamp in ISO 8601 format with millisecond accuracy: 2018-09-21T15:32:55.708.

Modified feature: Interface event

Feature change description

In this version and later, you can specify multiple interfaces of the same type for an interface event.

Command changes

Modified command: event interface

Old syntax

event interface *interface-type interface-number* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

New syntax

event interface *interface-list* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

Views

CLI-defined policy view

Parameters

interface-list: Specifies a space-separated list of up to eight interface items. An item specifies an interface or specifies a range of interfaces in the form of *interface-type interface-number* **to** *interface-type interface-number*. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

Change description

Before modification: Only one interface can be monitored.

After modification: Multiple interfaces can be monitored. The interfaces in an interface range must be same type. The start interface number must be smaller than the end interface number.

Modified feature: NTP

Feature change description

This release added support of maximum and minimum NTP polling intervals.

Command changes

Modified command: display ntp-service status

Syntax

display ntp-service status

Views

User view

Change description

Before modification: The command does not display the NTP polling interval.

After modification: The **System poll interval** field was added to the command output to display the NTP polling interval.

Modified command: ntp-service unicast-peer

Old syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

New syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

Modified command: ntp-service unicast-server

Old syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

New syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

Modified command: ntp-service ipv6 unicast-peer

Old syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

New syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

Modified command: ntp-service ipv6 unicast-server

Old syntax

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

New syntax

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to the command to allow for specifying the maximum and minimum NTP polling intervals.

Modified feature: Specifying the source IP address for NTP messages

Feature change description

You can configure the source IP address for NTP messages directly or by specifying an interface. Before the modification, the source IP address can be configured only by specifying an interface.

Command changes

Modified command: ntp-service source

Old syntax

ntp-service source *interface-type interface-number*

New syntax

ntp-service source { *interface-type interface-number* | *ip-address* }

Views

System view

Parameter

interface-type interface-number: Specifies an interface by its type and number. The device uses the primary address of the specified source interface as the source address to send NTP messages. The destination address of the NTP response messages is the primary address of the specified source interface.

ip-address: Specifies the source IP address for NTP messages.

Change description

The *ip-address* argument was added to the command.

Modified feature: sFlow counter sampling

Feature change description

In this version and later, you can specify an sFlow instance for counter sampling.

Command changes

Modified command: sflow counter collector

Old syntax

sflow counter collector *collector-id*

undo sflow counter collector

New syntax

sflow counter [**instance** *instance-id*] **collector** *collector-id*

undo sflow counter [**instance** *instance-id*] **collector**

Views

Layer 2 Ethernet interface view

Parameters

instance *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for counter sampling.

Change description

Before modification: You can specify only an sFlow collector for counter sampling.

After modification: You can specify an sFlow instance and an sFlow collector for counter sampling.

Modified feature: sFlow flow sampling

Feature change description

In this version and later, you can specify an sFlow instance for flow sampling.

Command changes

Modified command: sflow counter collector

Old syntax

sflow flow collector *collector-id*

undo sflow flow collector

New syntax

sflow flow [**instance** *instance-id*] **collector** *collector-id*

undo sflow flow [**instance** *instance-id*] **collector**

Views

Layer 2 Ethernet interface view

Parameters

instance *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for flow sampling.

Change description

Before modification: You can specify only an sFlow collector for flow sampling.

After modification: You can specify an sFlow instance and an sFlow collector for flow sampling.

Release 3208P16

This release has the following changes:

- New feature: Setting the block timer for MAC addresses in the blocked MAC address list
- New feature: Logging off 802.1X users
- New feature: Logging off MAC authentication users

New feature: Setting the block timer for MAC addresses in the blocked MAC address list

Setting the block timer for MAC addresses in the blocked MAC address list

About setting the block timer for MAC addresses in the blocked MAC address list

Use the block timer in conjunction with the intrusion protection action that blocks the source MAC addresses of illegal frames.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

Procedure

1. Enter system view.
   system-view
2. Set the block timer for blocked MAC addresses.
   port-security timer blockmac *time-value*
   By default, the block timer is 180 seconds.

Command reference

port-security timer blockmac

Use **port-security timer blockmac** to set the block timer for MAC addresses in the blocked MAC address list.

Use **undo port-security timer blockmac** to restore the default.

Syntax

port-security timer blockmac *time-value*

undo port-security timer blockmac

Default

The block timer for blocked MAC addresses is 180 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Sets a timer value in the range of 1 to 3600 seconds.

Usage guidelines

Use the block timer in conjunction with the intrusion protection action that blocks the source MAC addresses of illegal frames.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

Examples

Configure the intrusion protection action on GigabitEthernet 1/0/1 as blocking source MAC addresses of illegal frames, and set the block timer to 60 seconds.

```
<Sysname> system-view
[Sysname] port-security timer blockmac 60
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Related commands

display port-security

port-security intrusion-mode

New feature: Logging off 802.1X users

Logging off 802.1X users

About logging off 802.1X users

Perform this task to log off specific 802.1X users and clear information about these users from the device. These users must perform 802.1X authentication to come online again.

Procedure

To log off 802.1X users, execute the following command in user view:

reset dot1x access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Command reference

reset dot1x access-user

Use **reset dot1x access-user** to log off 802.1X users.

Syntax

reset dot1x access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac *mac-address*: Specifies an 802.1X user by its MAC address. The *mac-address* argument is in the format of H-H-H.

username *username*: Specifies an 802.1X user by its name. The *username* argument is a case-sensitive string of 1 to 253 characters.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Use this command to log off the specified 802.1X users and clear information about these users from the device. These users must perform 802.1X authentication to come online again.

If you specify a VLAN, this command logs off the following 802.1X users:

- Users that have passed 802.1X authentication and have been assigned the specified VLAN as the authorization VLAN.
- Users that have just passed 802.1X authentication and are to be assigned the specified VLAN as the authorization VLAN.
- Users that are performing 802.1X authentication in the specified VLAN.

If you do not specify any parameters, this command logs off all 802.1X users on the device.

Examples

Log off all 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x access-user interface gigabitethernet 1/0/1
```

Related commands

display dot1x connection

New feature: Logging off MAC authentication users

Logging off MAC authentication users

About logging off MAC authentication users

Perform this task to log off specific MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

Procedure

To log off MAC authentication users, execute the following command in user view:

reset mac-authentication access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Command reference

reset mac-authentication access-user

Use **reset mac-authentication access-user** to log off MAC authentication users.

Syntax

reset mac-authentication access-user [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

mac *mac-address*: Specifies a MAC authentication user by its MAC address. The *mac-address* argument is in the format of H-H-H.

username *username*: Specifies a MAC authentication user by its name. The *username* argument is a case-sensitive string of 1 to 253 characters.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Use this command to log off the specified MAC authentication users and clear information about these users from the device. These users must perform MAC authentication to come online again.

If you specify a VLAN, this command logs off the following MAC authentication users:

- Users that have passed MAC authentication and have been assigned the specified VLAN as their authorization VLAN.
- Users that have just passed MAC authentication and are to be assigned the specified VLAN as the authorization VLAN.
- Users that are performing MAC authentication in the specified VLAN.

If you do not specify any parameters, this command logs off all MAC authentication users on the device.

Examples

Log off all MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication access-user interface gigabitethernet 1/0/1
```

Related commands

display mac-authentication connection

Release 3208P15

This release has the following changes:

- New feature: Configuring zero-to-two VLAN mapping
- New feature: Specifying DNS server information in RA messages
- New feature: Specifying DNS suffix information in RA messages
- New feature: Suppressing advertising DNS information in RA messages
- New feature: HTTP redirect
- New feature: ERPS
- Modified feature: Physical type of a combo interface

New feature: Configuring zero-to-two VLAN mapping

Configuring zero-to-two VLAN mapping

About zero-to-two VLAN mapping

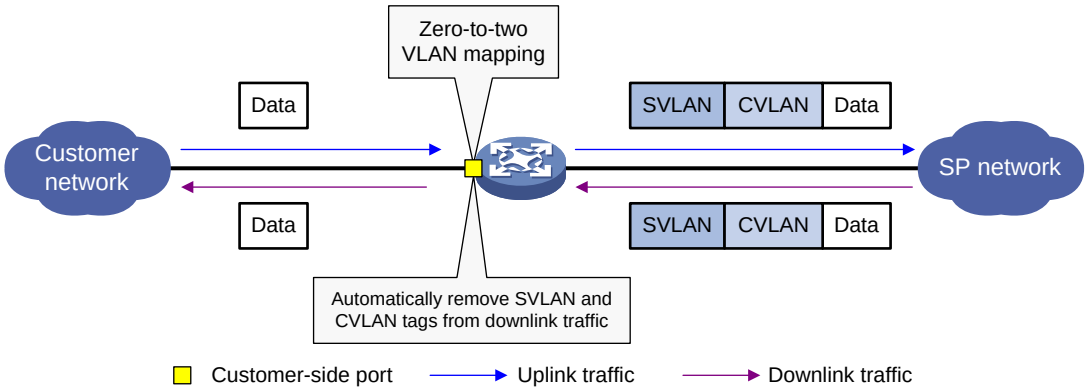
As shown in Figure 1, zero-to-two VLAN mapping is implemented on the customer-side port to add double tags to untagged uplink traffic. For zero-to-two VLAN mapping to take effect, the port PVID must be VLAN 1.

For correct downlink traffic transmission, the downlink traffic must be double-tagged. Then, the customer-side port removes both SVLAN and CVLAN tags from the traffic.

Use one of the following methods to ensure that the downlink traffic contains double tags on the customer-side port:

- Configure the port as a trunk port and assign it to the SVLAN, which must be different from the port PVID (VLAN 1).
- Configure the port as a hybrid port and assign it to the SVLAN as a tagged member.

Figure 1 Zero-to-two VLAN mapping implementation



Configuration restrictions and guidelines

As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

Procedure

1. Enter system view.

system-view

2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
3. Set the link type of the port.
   port link-type { **hybrid** | **trunk** }
   By default, the link type of a port is **access**.
4. Set the port PVID to VLAN 1.
   - Set the PVID to VLAN 1 for the trunk port.
     port trunk pvid vlan 1
   - Set the PVID to VLAN 1 for the hybrid port.
     port hybrid pvid vlan 1
5. Assign the port to the SVLAN and the port PVID (VLAN 1).
   - Assign the trunk port to the SVLAN and the port PVID (VLAN 1).
     port trunk permit vlan *vlan-id-list*
     By default, a trunk port is assigned to VLAN 1.
     The SVLAN of the trunk port must be different from the port PVID (VLAN 1).
   - Assign the hybrid port to the SVLAN and the port PVID (VLAN 1) as a tagged member.
     port hybrid vlan *vlan-id-list* **tagged**
     By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.
6. Configure a zero-to-two VLAN mapping.
   vlan mapping untagged nested-outer-vlan *outer-vlan-id* **nested-inner-vlan** *inner-vlan-id*
   By default, no VLAN mapping is configured on an interface.

Command reference

vlan mapping untagged

Use **vlan mapping untagged** to configure zero-to-two VLAN mapping on an interface.

Use **undo vlan mapping untagged** to remove the zero-to-two VLAN mapping configuration.

Syntax

vlan mapping untagged nested-outer-vlan *outer-vlan-id* **nested-inner-vlan** *inner-vlan-id*

undo vlan mapping untagged

Default

No zero-to-two VLAN mapping is configured on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

mdc-admin

Parameters

nested-outer-vlan *outer-vlan-id*: Specifies the SVLAN ID in the range of 1 to 4094.

nested-inner-vlan *inner-vlan-id*: Specifies the CVLAN ID in the range of 1 to 4094.

Usage guidelines

This command takes effect only on ports that use VLAN 1 as the PVID.

Before you modify a zero-to-two VLAN mapping, first execute the **undo vlan mapping untagged** command to remove the previous configuration.

As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

Examples

Configure a zero-to-two VLAN mapping on GigabitEthernet 1/0/1 to add SVLAN 200 and CVLAN 100 to untagged packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan mapping untagged nested-outer-vlan 200
nested-inner-vlan 100
```

New feature: Specifying DNS server information in RA messages

Specifying DNS server information in RA messages

About specifying DNS server information in RA messages

The DNS server options in RA messages provide DNS server information for IPv6 hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

After you execute the **ipv6 nd ra dns server** command, the device immediately sends an RA message with the existing and newly specified DNS server information.

After you execute the **undo ipv6 nd ra dns server** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS servers, including the DNS servers specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Restrictions and guidelines

You can configure a maximum of eight DNS servers on an interface.

The default lifetime of a DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Specify DNS server information to be advertised in RA messages.

   ipv6 nd ra dns server *ipv6-address* [*seconds* | **infinite**] **sequence** *seqno*

   By default, no DNS server information is specified and RA messages do not carry DNS server options.

Command reference

ipv6 nd ra dns server

Use **ipv6 nd ra dns server** to specify DNS server information to be advertised in RA messages.

Use **undo ipv6 nd ra dns server** to remove a DNS server from RA message advertisement.

Syntax

ipv6 nd ra dns server *ipv6-address* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns server *ipv6-address*

Default

DNS server information is not specified and RA messages do not carry DNS server options.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the DNS server, which must be a global unicast address or a link-local address.

seconds: Specifies the lifetime of the DNS server, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS server is infinite.

infinite: Sets the lifetime of the DNS server to infinite.

sequence *seqno*: Specifies the sequence number of the DNS server, in the range of 0 to 4294967295. The sequence number for a DNS server must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS server option in RA messages provides DNS server information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS server through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS server is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS servers on an interface. One DNS server option contains one DNS server. All DNS server options are sorted in ascending order of the DNS server sequence number.

The sequence number uniquely identifies a DNS server. To modify the IPv6 address or sequence number of a DNS server, you must first use the **undo ipv6 nd ra dns server** command to remove the DNS server from RA message advertisement.

After you execute the **ipv6 nd ra dns server** command, the device immediately sends an RA message with the existing and newly specified DNS server options.

After you execute the **undo ipv6 nd ra dns server** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS servers, including the DNS servers specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS servers.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS server address as **2001:10::100**, the server lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server 2001:10::100 infinite sequence 1
```

Related commands

- **ipv6 nd ra dns server suppress**
- **ipv6 nd ra interval**

New feature: Specifying DNS suffix information in RA messages

Specifying DNS suffix information in RA messages

About specifying DNS suffix information in RA messages

The DNSSL option in RA messages provides suffix information for IPv6 hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

After you execute the **ipv6 nd ra dns search-list** command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the **undo ipv6 nd ra dns search-list** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS suffixes, including DNS suffixes specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Restrictions and guidelines

You can configure a maximum of eight DNS suffixes on an interface.

The default lifetime of a DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Specify DNS suffix information to be advertised in RA messages.

   ipv6 nd ra dns search-list *domain-name* [*seconds* | **infinite**] **sequence** *seqno*

   By default, no DNS suffix information is specified and RA messages do not carry DNS suffix options.

Command reference

ipv6 nd ra dns search-list

Use **ipv6 nd ra dns search-list** to specify DNS suffix information to be advertised in RA messages.

Use **undo ipv6 nd ra dns search-list** to remove a DNS suffix from RA message advertisement.

Syntax

ipv6 nd ra dns search-list *domain-name* [*seconds* | **infinite**] **sequence** *seqno*

undo ipv6 nd ra dns search-list *domain-name*

Default

DNS suffix information is not specified and RA messages do not carry DNS suffix options.

Views

Interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a DNS suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The DNS suffix can include a maximum of 253 characters, and each separated string includes no more than 63 characters.

seconds: Specifies the lifetime of the DNS suffix, in seconds. The value range is 4 to 4294967295. Value 4294967295 indicates that the lifetime of the DNS suffix is infinite.

infinite: Sets the lifetime of the DNS suffix to infinite.

seqno: Specifies the sequence number of the DNS suffix, in the range of 0 to 4294967295. The sequence number for a DNS suffix must be unique. A smaller sequence number represents a higher priority.

Usage guidelines

The DNS search list (DNSSL) option in RA messages provides DNS suffix information for hosts. The RA messages allow hosts to obtain their IPv6 addresses and the DNS suffix through stateless autoconfiguration. This method is useful in a network where DHCPv6 infrastructure is not provided.

The default lifetime of the DNS suffix is three times the maximum interval for advertising RA messages. To set the maximum interval, use the **ipv6 nd ra interval** command.

You can configure a maximum of eight DNS suffixes on an interface. One DNSSL option contains one DNS suffix. All DNSSL options are sorted in ascending order of the sequence number of the DNS suffix.

The sequence number uniquely identifies a DNS suffix. To modify a DNS suffix or its sequence number, you must first use the **undo ipv6 nd ra dns search-list** command to remove the DNS suffix from RA message advertisement.

After you execute the **ipv6 nd ra dns search-list** command, the device immediately sends an RA message with the existing and newly specified DNS suffix information.

After you execute the **undo ipv6 nd ra dns search-list** command, the device immediately sends two RA messages.

- The first RA message carries information about all DNS suffixes, including DNS suffixes specified in the **undo** command with their lifetime set to 0 seconds.
- The second RA message carries information about remaining DNS suffixes.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Specify the DNS suffix as **com**, the suffix lifetime as **infinite**, and the sequence number as **1** for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list com infinite sequence 1
```

Related commands

- **ipv6 nd ra dns search-list suppress**
- **ipv6 nd ra interval**

New feature: Suppressing advertising DNS information in RA messages

Suppressing advertising DNS information in RA messages

About suppressing advertising DNS information in RA messages

Perform this task to suppress the device from advertising information about DNS server addresses and DNS suffixes in RA messages.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS server update depends on the interface configuration:

- If the interface has been configured with DNS server information, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not carry any DNS server options.
- If the interface has no DNS server information specified, no RA messages are triggered.
- If you specify a new DNS server or remove a DNS server, the device immediately sends an RA message without any DNS server address options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS server update depends on the interface configuration:

- If the interface has been configured with the DNS server information, the device immediately sends an RA message carrying the DNS server information.
- If the interface has no DNS server information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

The same suppression mechanism applies when you enable or disable DNS suffix suppression in RA messages.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Enable DNS server suppression in RA messages.

   ipv6 nd ra dns server suppress

   By default, DNS server suppression in RA messages is disabled.
4. Enable DNS suffix suppression in RA messages.

   ipv6 nd ra dns search-list suppress

   By default, DNS suffix suppression in RA messages is disabled.

Command reference

ipv6 nd ra dns search-list suppress

Use **ipv6 nd ra dns search-list suppress** to enable DNS suffix suppression in RA messages.

Use **undo ipv6 nd ra dns search-list suppress** to disable DNS suffix suppression in RA messages.

Syntax

ipv6 nd ra dns search-list suppress

undo ipv6 nd ra dns search-list suppress

Default

DNS suffix suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS suffixes in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

- If the interface has been configured with DNS suffix information, the device immediately sends two RA messages. In the first message, the lifetime for DNS suffixes is 0 seconds. The second RA message does not carry any DNSSL options.
- If the interface has no DNS suffix information specified, no RA messages are triggered.
- If you specify a new DNS suffix or remove a DNS suffix, the device immediately sends an RA message without any DNSSL options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS suffix update depends on the interface configuration:

- If the interface has been configured with the DNS suffix information, the device immediately sends an RA message carrying the DNS suffix information.
- If the interface has no DNS suffix information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS suffix suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns search-list suppress
```

Related commands

- **ipv6 nd ra dns search-list**

ipv6 nd ra dns server suppress

Use **ipv6 nd ra dns server suppress** to enable DNS server suppression in RA messages.

Use **undo ipv6 nd ra dns server suppress** to disable DNS server suppression in RA messages.

Syntax

ipv6 nd ra dns server suppress

undo ipv6 nd ra dns server suppress

Default

DNS server suppression in RA messages is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command suppresses advertising DNS server addresses in RA messages.

RA messages are suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Whether enabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

- If the interface has been configured with DNS server information, the device immediately sends two RA messages. In the first message, the lifetime for DNS server addresses is 0 seconds. The second RA message does not carry any DNS server options.
- If the interface has no DNS server information specified, no RA messages are triggered.
- If you specify a new DNS server or remove a DNS server, the device immediately sends an RA message without any DNS server address options.

Whether disabling this feature on an interface will trigger sending RA message immediately for DNS server information update depends on the interface configuration:

- If the interface has been configured with the DNS server information, the device immediately sends an RA message carrying the DNS server information.
- If the interface has no DNS server information specified, no RA messages are triggered.

Each time the device sends an RA message from an interface, it immediately refreshes the RA message advertisement interval for that interface.

Examples

Enable DNS server suppression in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra dns server suppress
```

Related commands

- **ipv6 nd ra dns server**

New feature: HTTP redirect

About HTTP redirect

HTTP redirect is a method to redirect users' HTTP or HTTPS requests to a specific URL. It is used in the following features:

- Redirect URL assignment in 802.1X authentication, MAC authentication, and port security.
- EAD assistant URL redirection in 802.1X authentication.
- URL redirection services in portal.

HTTP redirect tasks at a glance

No configuration is required to redirect HTTP requests.

To redirect HTTPS requests, perform the following tasks:

1. Specifying the HTTPS redirect listening port number
2. (Optional.) Associating an SSL server policy with the HTTPS redirect service

Specifying the HTTPS redirect listening port number

About the HTTPS redirect listening port number

The device can redirect HTTPS requests only after you specify the TCP port number on which the HTTPS redirect service listens for HTTPS requests.

Restrictions and guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other TCP-based service. To display TCP port numbers that have been used by services, use the **display tcp** command. For more information about this command, see IP performance optimization commands in *Layer 3—IP Services Command Reference*.

If you perform this task multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.

   system-view

2. Specify the HTTPS redirect listening port number.

   http-redirect https-port *port-number*

   By default, no HTTPS redirect listening port number is specified.

Associating an SSL server policy with the HTTPS redirect service

About associating an SSL server policy with the HTTPS redirect service

To improve the security of HTTPS redirect, you can associate an SSL server policy with the HTTPS redirect service. For more information about the SSL server policy configuration, see SSL in *Security Configuration Guide*.

Restrictions and guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.

   system-view

2. Associate an SSL server policy with the HTTPS redirect service.

   http-redirect ssl-server-policy *policy-name*

   By default, no SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses the self-assigned certificate and the default SSL parameters.

Command reference

http-redirect https-port

Use **http-redirect https-port** to specify the HTTPS redirect listening port number.

Use **undo http-redirect https-port** to restore the default.

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

Default

No HTTPS redirect listening port number is specified.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the TCP port number on which the HTTPS redirect service listens for HTTPS requests. The value range for the port number is 1 to 65535.

Usage guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other service. To display TCP port numbers that have been used by services, use the **display tcp** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify 8888 as the HTTPS redirect listening port number.

```
<Sysname> system-view
[Sysname] http-redirect https-port 8888
```

http-redirect ssl-server-policy

Use **http-redirect ssl-server-policy** to associate an SSL server policy with the HTTPS redirect service.

Use **undo http-redirect ssl-server-policy** to restore the default.

Syntax

http-redirect ssl-server-policy *policy-name*

undo http-redirect ssl-server-policy

Default

No SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses a self-assigned certificate and the default SSL parameters.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Examples

Associate SSL server policy **policy1** with the HTTPS redirect service.

```
<Sysname> system-view
[Sysname] http-redirect ssl-server-policy policy1
```

Related commands

ssl server-policy

New feature: ERPS

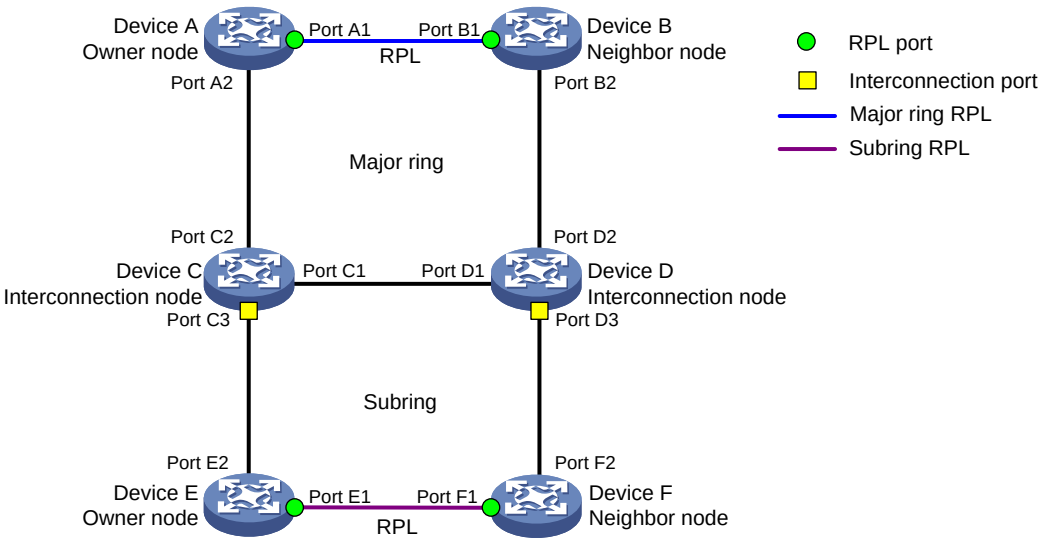
Configuring ERPS

About ERPS

Ethernet Ring Protection Switching (ERPS) is a robust link layer protocol that ensures a loop-free topology and implements quick link recovery.

ERPS structure

Figure 2 ERPS ring structure



Rings

ERPS rings can be divided into major rings and subrings. An ERPS network consists of one major ring or multiple major rings, and multiple subrings. By default, a ring is a major ring. You can configure a ring as a subring manually.

As shown in Figure 2, a major ring is a closed ring formed by Device A, Device B, Device C, and Device D. A subring is an open ring formed by the link Device C<—>Device E<—>Device F<—>Device D.

RPL

An ERPS ring is composed of many nodes. Some nodes use ring protection links (RPLs) to prevent loops on the ERPS ring. As shown in Figure 2, the link between Device A and Device B and the link between Device E and Device F are RPLs.

Nodes

ERPS nodes include owner nodes, neighbor nodes, interconnection nodes, and normal nodes.

- The owner node and neighbor node block and unblock ports on the RPL to prevent loops and switch traffic. An RPL connects an owner node and a neighbor node.
- Interconnection nodes connect different rings. Interconnection nodes reside on subrings and forward service packets but not protocol packets.
- Normal nodes forward both service packets and protocol packets.

As shown in Figure 2, on the major ring, Device A is the owner node and Device B is the neighbor node. On the subring, Device E is the owner node and Device F is the neighbor node. Devices C and D are interconnection nodes.

Ports

Each node consists of two ERPS ring member ports: Port 0 and port 1. ERPS ring member ports have the following types:

- **RPL port**—Port on an RPL link.
- **Interconnection port**—Port that connects a subring to a major ring.
- **Normal port**—Default type of a port that forwards both service packets and protocol packets.

As shown in Figure 2, ports A1, B1, E1, and F1 are RPL ports. Ports C3 and D3 are interconnection ports. Other ports are normal ports.

Instances

An ERPS ring supports multiple ERPS instances. An ERPS instance is a logical ring to process service and protocol packets. Each ERPS instance has its own owner node and maintains its own state and data. An ERPS instance is uniquely identified by the ring ID and VLAN ID of ERPS packets. The ring ID indicates the ring of ERPS packets. It can be represented by the last byte in the destination MAC address of the packets. The VLAN ID indicates the ERPS instance of the packets.

ERPS protocol packets

ERPS protocol packets are Ring Automatic Protection Switching (R-APS) packets. You can configure the R-APS packet level. A node does not process R-APS packets whose levels are greater than the level of the packets sent by the node. On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

Table 1 R-APS packet types and functions

Packet type	Function
No request, RPL block (NR-RB)	When the link is stable, an owner node in idle state periodically sends NR-RB packets to inform other nodes that the RPL ports are blocked. The nodes that receive the NR-RB packets unblock available ports and update MAC address entries.
No request (NR)	After the link fault is cleared, the node that detects the recovery periodically sends NR packets. When the owner node receives the NR packets, it starts the WTR timer. The node stops sending NR packets after receiving NR-RB packets from the owner node.
Signal fail (SF)	When a link fails to send or receive signals, the node that detects the fault

Packet type	Function
	periodically sends SF packets. When the owner node and neighbor node receive the FS packets, they unblock the RPL ports. The node stops sending SF packets after the fault is cleared.
Manual switch (MS)	A port configured with the MS mode is blocked and periodically sends MS packets. When other nodes receive the MS packets, they unblock available ports and update MAC address entries.
Forced switch (FS)	A port configured with the FS mode is blocked and periodically sends FS packets. When other nodes receive the FS packets, they unblock all ports and update MAC address entries.
Flush	If the topology of a subring changes, the interconnection ports on the subring broadcasts flush packets. All nodes that receive the flush packets update MAC address entries.

NOTE:

- Typically R-APS packets are transmitted within a ring. The flush packets sourced from the subring can be forwarded to the major ring.
- Service packets can be transmitted between different rings.

ERPS node states

Table 2 ERPS states

State	Description
Init	State for a non-interconnection node that has less than two ERPS ring member ports or for an interconnection node that does not have ERPS ring member ports.
Idle	Stable state when all non-RPL links are available. In this state, the owner node blocks the RPL port and periodically sends NR-RB packets. The neighbor node blocks the RPL port. All nodes enter the idle state after the owner node enters the idle state.
Protection	State when a non-RPL link is faulty. In this state, the RPL link is unblocked to forward traffic. All nodes enter the protection state after a node enters the protection state.
MS	State when traffic paths are manually switched. All nodes enter the MS state after a node is configured with the MS mode.
FS	State when traffic paths are forcibly switched. All nodes enter the FS state after a node is configured with the FS mode.
Pending	Transient state between the previous states.

ERPS timers

Hold-off timer

The hold-off timer starts when the port detects a link fault. The port reports the link fault if the fault persists when the timer expires.

This timer delays the fault report time and affects the link switching performance.

Guard timer

The guard timer starts when the port detects a link recovery. The port does not process R-APS packets before the timer expires.

This timer prevents R-APS packets from impacting the network and affects the link switching performance when multiple points of failures exist.

WTR timer

In revertive mode, the WTR timer starts when the owner node in protection state receives NR packets. The RPL is unblocked and the recovered node is blocked before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.

This timer prevents intermittent link failures from impacting the network.

WTB timer

In revertive mode, the WTB timer starts when the owner node in MS or FS state receives NR packets. The RPL is unblocked and the recovered node sends NR packets before the timer expires. The owner node blocks the RPL and sends NR-RB packets when the timer expires. If the port receives SF packets before the timer expires, the timer stops and the RPL remains unblocked.

This timer prevents the RPL ports from being blocked and unblocked frequently.

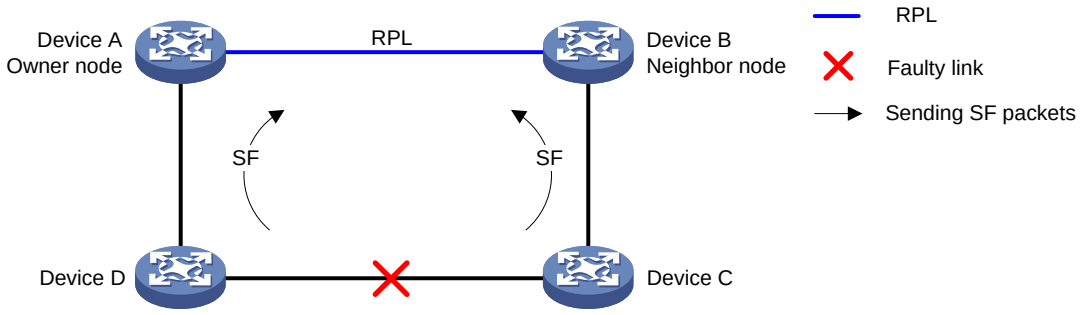
ERPS operation mechanism

ERPS uses the detection mechanism defined in ITU-T G.8032/Y.1344 to locate the point of failure and identify unidirectional or bidirectional faults.

ERPS uses the SF packets to report signal failures on a link and the NR packets to report link recovery. When a node detects a link status change, the node sends three packets first and then sends subsequent packets every five seconds.

Link-down report mechanism

Figure 3 Link-down report mechanism



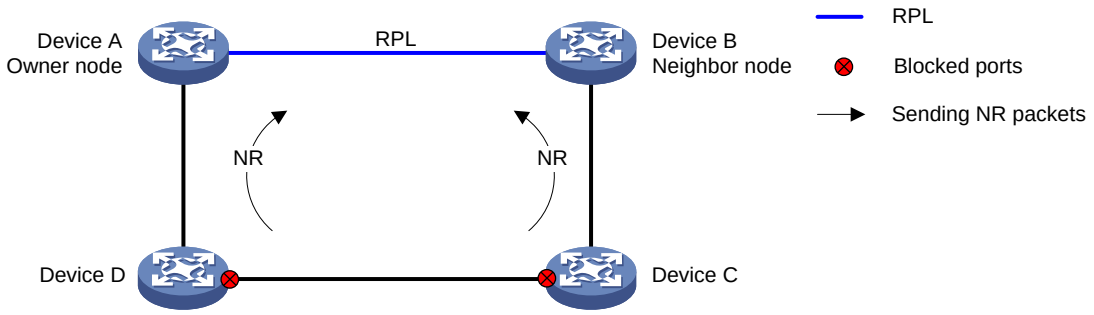
As shown in Figure 3, the link-down report mechanism uses the following process:

2. Device C and Device D detect the link failure and perform the following operations:
   a. Block the ports on both side of the faulty link.
   b. Periodically send SF packets to other nodes.
3. Device A and Device B receive the SF packets and perform the following operations:
   a. Unblock RPL ports.
   b. Update the MAC address entries.

Service packets are switched to the RPL link.

Link recovery mechanism

Figure 4 Link recovery mechanism



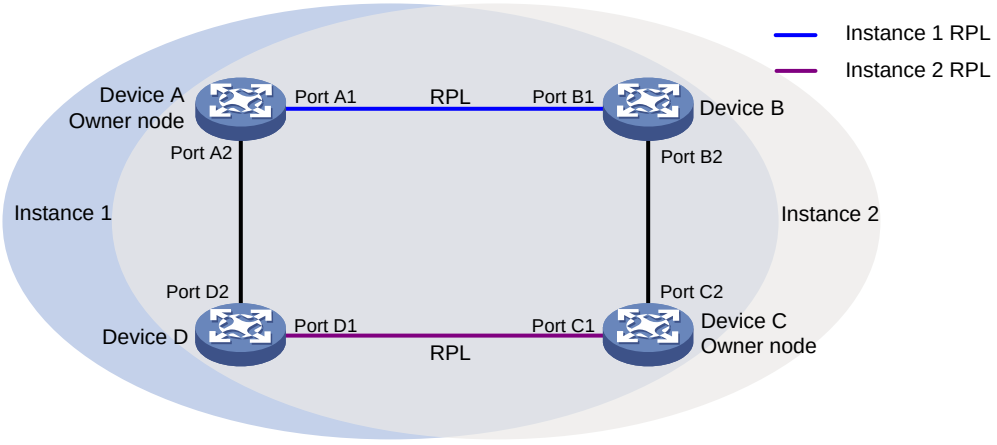
As shown in Figure 4, the link recovery mechanism uses the following process:

4. Device C and Device D detect the link recovery and perform the following operations:
   a. Block the recovered ports.
   b. Start the guard timer.
   c. Send NR packets.
5. When Device A (owner node) receives the NR packets, it does not perform any operations if it is in non-revertive mode. If Device A is in revertive mode, it performs the following operations:
   a. Starts the WTR timer.
   b. Blocks the RPL port and periodically sends NR-RB packets when the WTR timer expires.
6. When other nodes receive the NR-RB packets, they perform the following operations:
   a. Device B (neighbor port) blocks the RPL port.
   b. Device C and Device D unblock the recovered ports.

Service packets are switched to the recovered link.

Multi-instance load balancing mechanism

Figure 5 Multi-instance load balancing mechanism



An ERPS ring topology might carry traffic from multiple VLANs. Traffic from different VLANs can be load balanced among different ERPS instances.

ERPS uses the following types of VLANs:

- **Control VLAN**—Carries ERPS protocol packets. Each ERPS instance has its own control VLAN.
- **Protected VLAN**—Carries data packets. Each ERPS instance has its own protected VLAN. Protected VLANs are configured by using the mappings between VLANs and MSTIs.

As shown in Figure 5, the ERPS ring is configured with instance 1 and instance 2. For instance 1, the owner node is Device A, and the RPL is the link between Device A and Device B. For instance 2, the owner node is Device C, and the RPL is the link between Device C and Device D. Traffic from different VLANs can be load balanced among different links.

Manual configuration mechanism

ERPS supports the following manual configuration modes:

- **MS**—Use the **`erps switch manual`** command to block an ERPS ring member port. A port in MS mode is blocked and sends MS packets. The nodes that receive the MS packets unblock available ports. If the nodes in MS mode receive an SF packet, they unblock the blocked ports.
- **FS**—Use the **`erps switch force ring`** command to block an ERPS ring member port. A port in FS mode is blocked and sends FS packets. The nodes that receive the FS packets unblock available ports. If the nodes in FS mode receive an SF packet, they do not unblock the blocked ports.

Collaboration mechanism

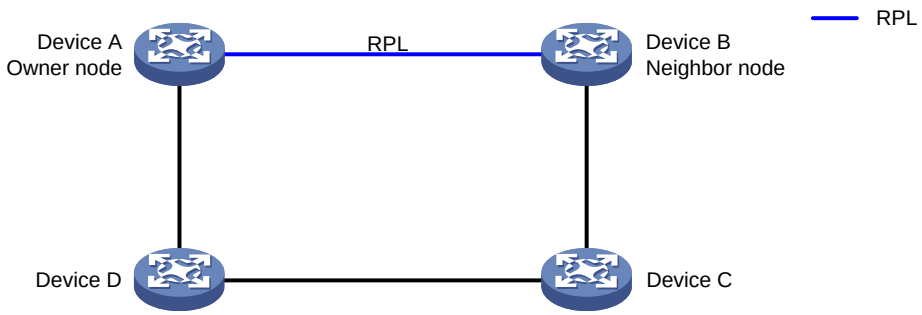
To detect and clear link faults typically for a fiber link, use ERPS with CFD and Track. You can associate ERPS ring member ports with the continuity check function of CFD through track entries. CFD reports link events only when the monitored VLAN is the control VLAN of the ERPS instance for the port. For more information about CFD and Track, see "Configuring CFD" and "Configuring Track."

ERPS network diagrams

One major ring

The network has one major ring.

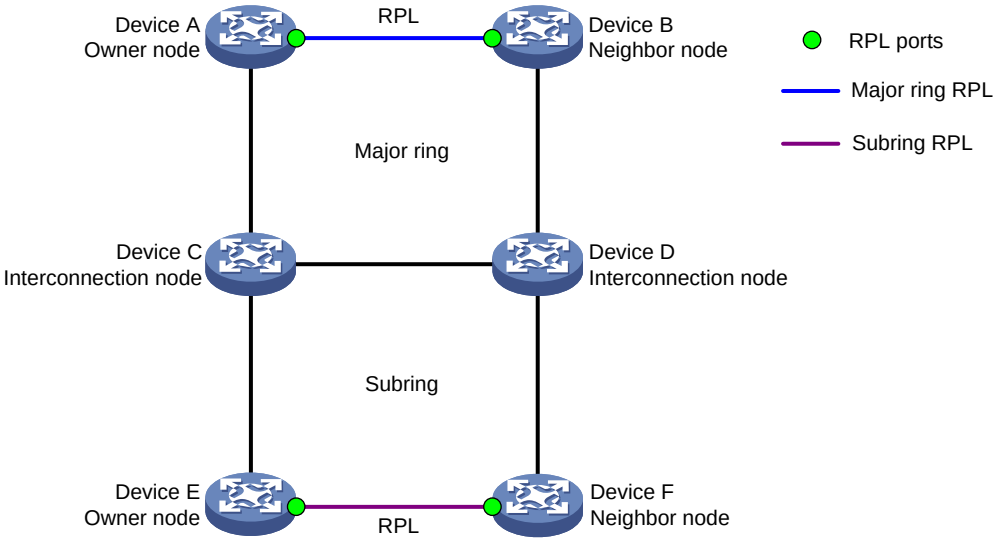
Figure 6 Network diagram



One major ring connecting one subring

The network has one major ring and one subring.

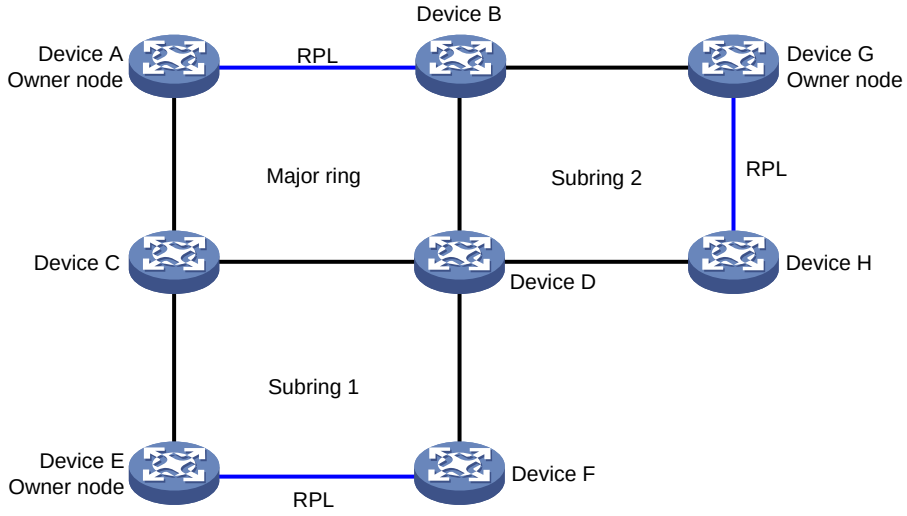
Figure 7 Network diagram



One major ring connecting multiple subrings

The network has three or more rings. Each subring is connected to the major ring by two interconnection nodes.

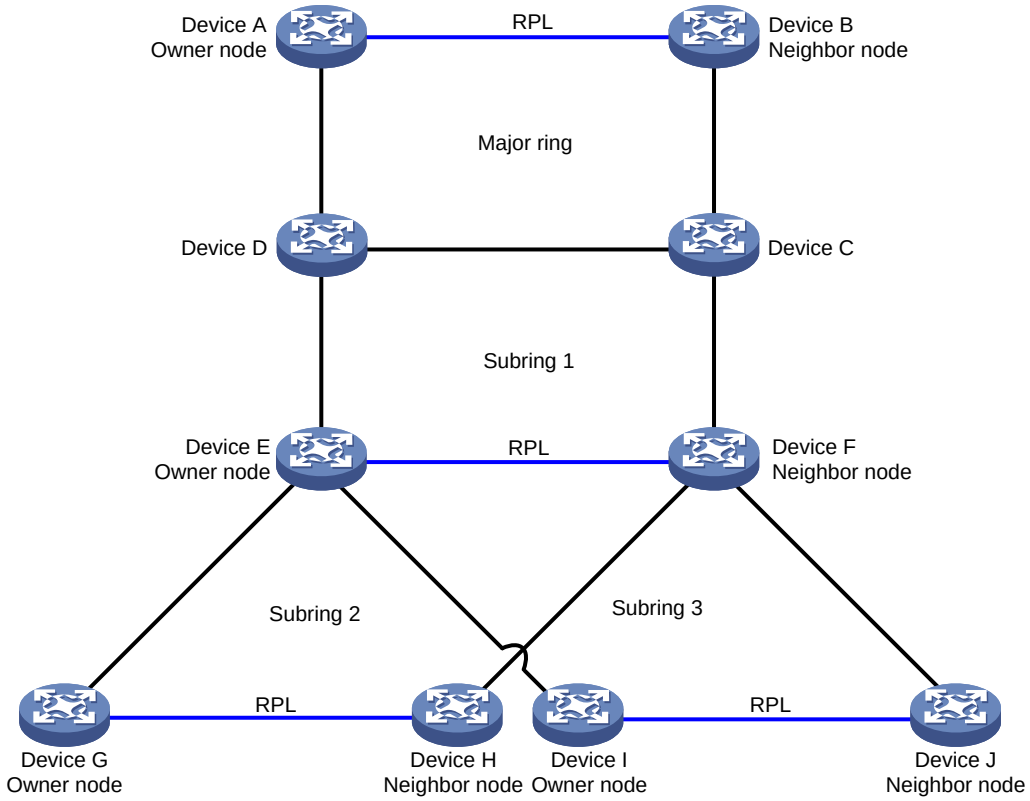
Figure 8 Network diagram



One subring connecting multiple subrings

The network has three or more rings. As shown in Figure 9, subring 1 is connected to the major ring. Other subrings are connected to subring 1 by two interconnection nodes.

Figure 9 Network diagram



One subring connecting multiple rings

The network has three or more rings. A minimum of one subring is connected to two rings. As shown in Figure 10, one interconnection node on subring 2 is connected to the major ring; and another interconnection node is connected to subring 1. As shown in Figure 11, subring 3 is connected to subring 1 and subring 2.

Figure 10 Network diagram 1

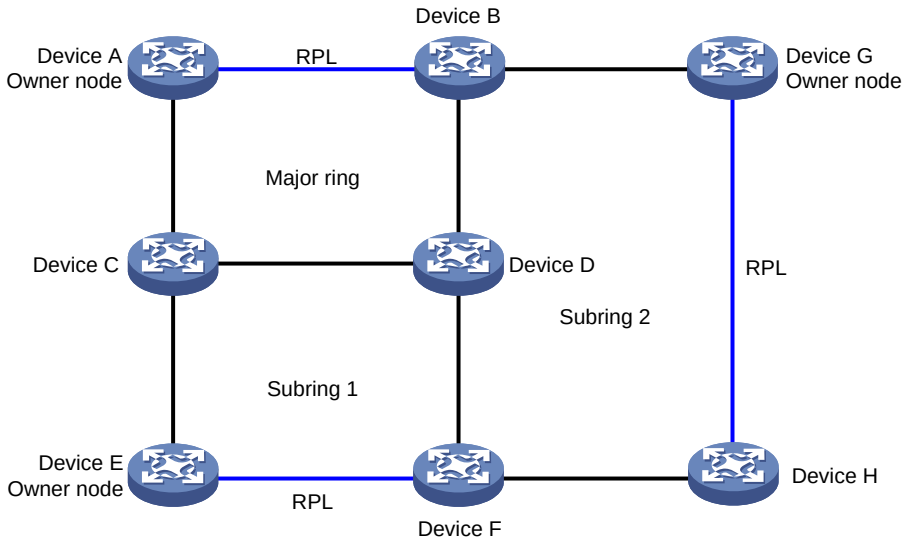
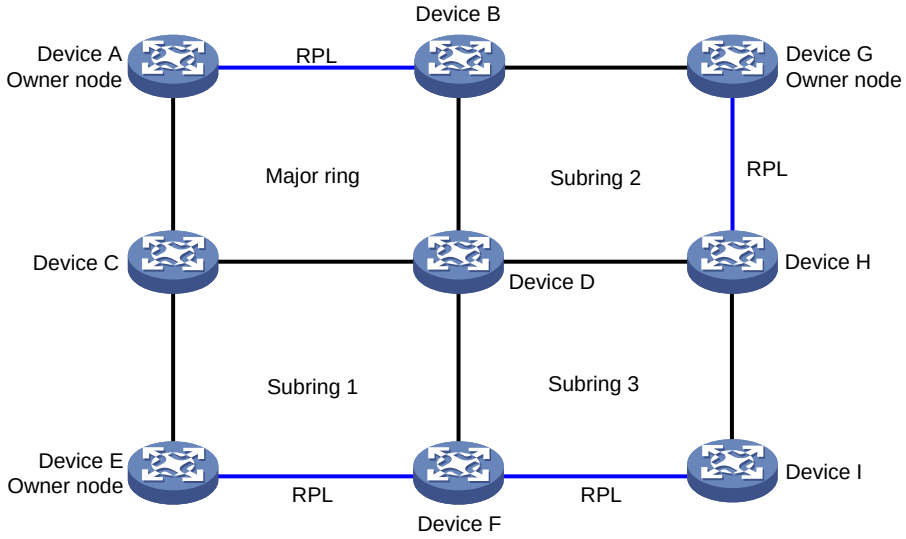


Figure 11 Network diagram 2



Protocols and standards

- ITU-T G.8032, *Recommendation ITU-T G.8032/Y.1344, Ethernet ring protection switching*
- IEEE 802.1D, *IEEE Std 802.1D™-2004, IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges*
- IEEE 802.3, *IEEE Std 802.3-2008, IEEE Standard for Information technology*

Restrictions and guidelines: ERPS configuration

ERPS does not provide an election mechanism. To implement ring detection and protection, configure all nodes correctly.

ERPS tasks at a glance

To configure ERPS, perform the following tasks:

1. Enabling ERPS globally

   Perform this task on devices you want to configure as ERPS nodes.
2. Configuring an ERPS ring

   Perform this task on all nodes on an ERPS ring.
   a. Creating an ERPS ring
   b. Configuring ERPS ring member ports
   c. Configuring control VLANs
   d. Configuring protected VLANs
   e. Configuring the node role
3. Enabling ERPS for an instance

   Perform this task on all nodes on an ERPS ring.
4. (Optional.) Enabling R-APS packets to carry the ring ID in the destination MAC address

   Perform this task on all nodes on an ERPS ring.
5. (Optional.) Configuring R-APS packet levels
6. (Optional.) Setting ERPS timers

   Perform this task on the owner node on an ERPS ring.

7. (Optional.) Setting the non-revertive mode

   Perform this task on the owner node on an ERPS ring.
8. (Optional.) Setting a switchover mode

   Perform this task on the nodes that you want to block their ports.
9. (Optional.) Associating a ring with a subring

   Perform this task on the interconnection node on an ERPS ring.
10. (Optional.) Enabling flush packet transparent transmission

    Perform this task on the interconnection node on an ERPS ring.
11. (Optional.) Associating an ERPS ring member port with a track entry
12. (Optional.) Removing the MS mode and FS mode settings for an ERPS ring

Prerequisites

Before you configure ERPS, complete the following tasks:

- Establish the Ethernet ring topology.
- Determine the ERPS rings, ERPS instances, control VLANs, protected VLANs, and node roles.

Enabling ERPS globally

Restrictions and guidelines

- Perform this task on devices you want to configure as ERPS nodes.
- For ERPS to take effect for an instance, enable it globally first.

Procedure

1. Enter system view.

   system-view
2. Enable ERPS globally.

   erps enable

   By default, ERPS is disabled globally.

Configuring an ERPS ring

Creating an ERPS ring

Restrictions and guidelines

- Perform this task on all nodes on an ERPS ring.
- A ring ID uniquely identifies an ERPS ring. All nodes on an ERPS ring must be configured with the same ring ID.

Procedure

1. Enter system view.

   system-view
2. Create an ERPS ring.

   erps ring *ring-id*
3. (Optional.) Configure the ring type.

   ring-type sub-ring

   By default, an ERPS ring is a major ring.

Configuring ERPS ring member ports

Restrictions and guidelines

- Perform this task on each node's ports intended for accessing ERPS rings.
- ERPS ring member ports automatically allow packets from the control VLAN to pass through.
- Do not enable Ethernet OAM remote loopback for ERPS ring member ports. This feature might cause a broadcast storm. For more information about Ethernet OAM, see "Configuring Ethernet OAM."
- For faster topology convergence, use the **link-delay** command on ERPS ring member ports to set the physical state change suppression interval to 0 seconds. For more information about the **link-delay** command, see *Interface Command Reference*.
- You must configure ERPS ring member ports as trunk ports.
- Do not assign an interface to both an aggregation group and an ERPS ring. If you do so, the interface does not take effect on the ERPS ring and cannot be displayed by using the **display erps detail** command.

Configuring ERPS ring member port attributes

1. Enter system view.

   system-view
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.

   interface *interface-type interface-number*
3. Configure the port as a trunk port.

   port link-type trunk

   By default, a port is an access port.

   For more information about this command, see *Layer 2—LAN Switching Command Reference*.
4. Assign the trunk port to protected VLANs.

   port trunk permit vlan { *vlan-id-list* | **all** }

   By default, a trunk port is assigned only to VLAN 1.

   For more information about this command, see *Layer 2—LAN Switching Command Reference*.
5. Disable the spanning tree feature.

   undo stp enable

   By default, the spanning tree feature is enabled.

   For more information about this command, see *Layer 2—LAN Switching Command Reference*.

Configuring an ERPS ring member port

1. Enter system view.

   system-view
2. Enter ERPS ring view.

   erps ring *ring-id*
3. Configure an ERPS ring member port.

   { **port0** | **port1** } **interface** *interface-type interface-number*

   By default, an ERPS ring does not have ERPS ring member ports.

Configuring control VLANs

Restrictions and guidelines

- Perform this task on all nodes on an ERPS ring.
- The control VLAN must be a VLAN that has not been created on the device.

- Configure the same control VLAN for all nodes in an ERPS instance.
- Do not configure the default VLAN of an ERPS ring member port as the control VLAN.
- Do not enable QinQ or VLAN mapping on control VLANs. If you do, ERPS packets cannot be correctly forwarded and received.
- Make sure the ERPS instance has been configured. After the ERPS instance is enabled, the control VLAN cannot be changed.
- For a device not configured with ERPS to transparently transmit ERPS packets, make sure only the two ports accessing the ERPS ring permit packets from the control VLAN. If other ports on the device permit packets from the control VLAN, the packets from other VLANs might enter the control VLAN and strike the ERPS ring.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enable ERPS instance view.
   instance *instance-id*
4. Configure a control VLAN.
   control-vlan *vlan-id*

Configuring protected VLANs

Restrictions and guidelines

- Perform this task on all nodes on an ERPS ring.
- Configure the same protected VLAN for all nodes of an ERPS instance. To implement load balancing, configure different protected VLANs for different ERPS instances.

Prerequisites

Before you configure protected VLANs, you must configure an MST region and the VLAN-to-instance mapping table. For more information about MST regions, see spanning tree configuration in *Layer 2—LAN Switching Configuration Guide*.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enable ERPS instance view.
   instance *instance-id*
4. Configure the protected VLANs.
   protected-vlan reference-instance *instance-id-list*

Configuring the node role

Restrictions and guidelines

- Perform this task on all nodes on an ERPS ring.
- For the owner node to work correctly, you must configure only one owner node for an ERPS ring.
- You can only configure the interconnection node for subrings.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enter ERPS instance view.
   instance *instance-id*
4. Configure the node role.
   node-role { { **owner** | **neighbor** } **rpl** | **interconnection** } { **port0** | **port1** }
   By default, a node is a normal node.

Enabling ERPS for an instance

Restrictions and guidelines

- Perform this task on all nodes on an ERPS ring.
- You can enable ERPS for an instance only when it is configured with a control VLAN and a protected VLAN.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enter ERPS instance view.
   instance *instance-id*
4. Enable ERPS for the instance.
   instance enable
   By default, ERPS is disabled for an instance.

Enabling R-APS packets to carry the ring ID in the destination MAC address

About this feature

Perform this task to configure the ring ID as the last byte of the destination MAC address for R-APS packets. The ring of R-APS packets can be identified by their destination MAC addresses.

Restrictions and guidelines

Perform this task on all nodes on an ERPS ring.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enable R-APS packets to carry the ring ID in the destination MAC address.
   r-aps ring-mac
   By default, R-APS packets do not carry ring IDs in their destination MAC addresses. The last byte of the destination MAC address is 1.

Configuring R-APS packet levels

Restrictions and guidelines

Perform this task on all nodes on an ERPS ring.

On a ring, the levels of R-APS packets must be the same for all nodes in an ERPS instance.

A node does not process R-APS packets whose levels are greater than the level of R-APS packets sent by the node.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enter ERPS instance view.
   instance *instance-id*
4. Configure the R-APS packet level.
   r-aps level *level-value*
   By default, the level for R-APS packets is 7.

Setting ERPS timers

Restrictions and guidelines

Perform this task on the owner node on an ERPS ring.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enter ERPS instance view.
   instance *instance-id*
4. Set the guard timer.
   timer guard *guard-value*
   By default, the guard timer is 500 milliseconds.
5. Set the hold-off timer.
   timer hold-off *hold-off-value*
   By default, the hold-off timer is 0 milliseconds.
6. Set the WTR timer.
   timer wtr *wtr-value*
   By default, the WTR timer is 5 minutes.

Setting the non-revertive mode

About setting the non-revertive mode

Perform this task if you do not want to switch back to the recovered link after the link fault is cleared.

Restrictions and guidelines

Perform this task on the owner node on an ERPS ring.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Enter ERPS instance view.
   instance *instance-id*
4. Set the non-revertive mode.
   revertive-operation non-revertive
   By default, revertive mode is used.

Setting a switchover mode

Restrictions and guidelines

Perform this task on the nodes that you want to block their ports.

Procedure

1. Enter system view.
   system-view
2. Set a switchover mode.
   erps switch { **force** | **manual** } **ring** *ring-id* **instance** *instance-id* { **port0** | **port1** }
   By default, no switchover mode is not set.

Associating a ring with a subring

About associating a ring with a subring

On a multi-ring network, perform this task if you want to advertise topology changes in a subring to a ring.

Restrictions and guidelines

Perform this task on the interconnection node on an ERPS ring.

Procedure

1. Enter system view.
   system-view
2. Enter ERPS ring view.
   erps ring *ring-id*
3. Configure the ERPS ring as a subring.
   ring-type sub-ring
   By default, an ERPS ring is a major ring.
4. Enter ERPS instance view.
   instance *instance-id*
5. Associate a ring with the subring.
   sub-ring connect ring *ring-id* **instance** *instance-id*
   By default, a subring is not associated with any rings.

Enabling flush packet transparent transmission

About enabling flush packet transparent transmission

This feature enables the interconnection nodes to forward flush packets for topology changes in the subring to the ring associated with the subring. The associated ring can flush the MAC address table quickly to speed up convergence.

Restrictions and guidelines

Perform this task on the interconnection node on an ERPS ring.

To use this feature, you must also associate a subring on the interconnection node with the ring.

Procedure

1. Enter system view.
   system-view
2. Enable flush packet transparent transmission.
   erps tcn-propagation
   By default, flush packet transparent transmission is disabled.

Associating an ERPS ring member port with a track entry

Restrictions and guidelines

Before you associate a port with a track entry, make sure the port has joined an ERPS instance.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.
   interface *interface-type interface-number*
3. Associate an ERPS ring member port with a track entry.
   port erps ring *ring-id* **instance** *instance-id* **track** *track-entry-index*
   By default, an ERPS ring member port is not associated with any track entries.

Removing the MS mode and FS mode settings for an ERPS ring

About removing the MS mode and FS mode settings

After you configure this task, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This task also switches an ERPS ring in non-revertive mode to revertive mode.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.
   erps clear ring *ring-id* **instance** *instance-id*

Displaying and maintaining ERPS

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display brief ERPS information.	**display erps**
Display detailed ERPS information.	**display erps detail ring** *ring-id* [**instance** *instance-id*]
Display ERPS packet statistics.	**display erps statistics** [**ring** *ring-id* [**instance** *instance-id*]]
Clear ERPS packet statistics.	**reset erps statistics ring** *ring-id* [**instance** *instance-id*]

ERPS configuration examples

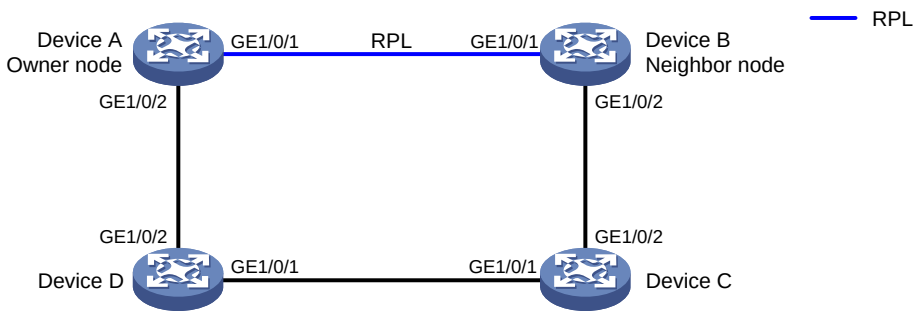
Example: Configuring one ring

Network configuration

As shown in Figure 12, perform the following tasks to eliminate loops on the network:

- Configure the ring as ERPS ring 1.
- Configure VLAN 100 as the control VLAN for ERPS ring 1.
- Configure VLANs 1 to 30 as the protected VLANs for ERPS ring 1.
- Configure Device A as the owner node, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device B as the neighbor node, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device C and Device D as normal nodes, GigabitEthernet 1/0/1 as ERPS ring member port 0, and GigabitEthernet 1/0/2 as ERPS ring member port 1.

Figure 12 Network diagram



Procedure

2. Configure Device A.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceA] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Enable R-APS packets to carry ring ID in the destination MAC address.

```
[DeviceA-erps-ring1] r-aps ring-mac
```

Create ERPS instance 1.

```
[DeviceA-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
```

Configure the control VLAN.

```
[DeviceA-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

```
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

```
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
```

Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceA] erps enable
```

3. Configure Device B.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceB] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Enable R-APS packets to carry ring ID in the destination MAC address.

```
[DeviceB-erps-ring1] r-aps ring-mac
```

Create ERPS instance 1.

```
[DeviceB-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
```

Configure the control VLAN.

```
[DeviceB-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

```
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
```

Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

```
[DeviceB] track 3 cfd cc service-instance 3 mep 3002
```

Associate GigabitEthernet 1/0/2 with track entry 3 and bring up the port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceB] erps enable
```

4. Configure Device C.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceC] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Enable R-APS packets to carry ring ID in the destination MAC address.

```
[DeviceC-erps-ring1] r-aps ring-mac
```

Create ERPS instance 1.

```
[DeviceC-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceC-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

```
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

```
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
```

Associate GigabitEthernet 1/0/1 with track entry 3 and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/1
```

```
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceC] erps enable
```

5. Configure Device D.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceD] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Enable R-APS packets to carry ring ID in the destination MAC address.

```
[DeviceD-erps-ring1] r-aps ring-mac
```

Create ERPS instance 1.

```
[DeviceD-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceD-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

```
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

```
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceD] erps enable
```

Verifying the configuration

Display information about ERPS instance 1 for Device A.

```
[DeviceA] display erps detail ring 1
 Ring ID               : 1
 Port0                 : GigabitEthernet1/0/1
 Port1                 : GigabitEthernet1/0/2
 Subring               : No
```

```
Default MAC           : No
Instance ID           : 1
Node role             : Owner
Node state            : Idle
Connect(ring/instance): -
Control VLAN          : 100
Protected VLAN        : Reference-instance 1
Guard timer           : 500 ms
Hold-off timer        : 0 ms
WTR timer             : 5 min
Revertive operation   : Revertive
Enable status         : Yes, Active status : Yes
R-APS level           : 7
Port                  PortRole                PortStatus
--------------------------------------------------------------------------------
Port0                 RPL                     Block
Port1                 Non-RPL                 Up
```

The output shows the following information:

- Device A is the owner node.
- The ERPS ring is in idle state.
- The RPL port is blocked.
- The non-RPL port is unblocked.

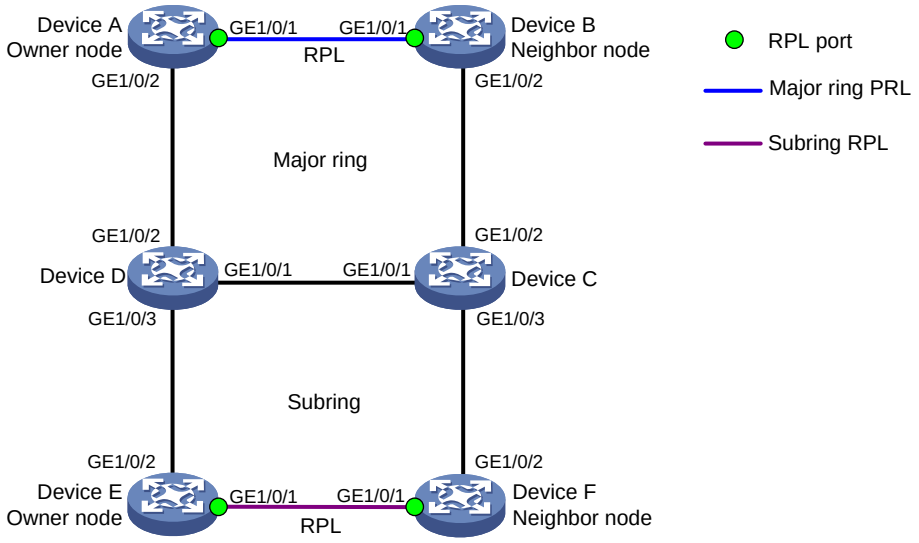
Example: Configuring one subring

Network configuration

As shown in Figure 13, perform the following tasks to eliminate loops on the network:

- Configure VLAN 100 and VLAN 200 as the control VLANs for the major ring and the subring, respectively.
- Configure VLANs 1 to 30 as the protected VLANs for the major ring and subring.
- Configure Device A as the owner node for the major ring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device B as the neighbor node for the major ring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Devices C and D as interconnection nodes, GigabitEthernet 1/0/1 as ERPS ring member port 0, GigabitEthernet 1/0/2 as ERPS ring member port 1, and GigabitEthernet 1/0/3 as the interconnection port.
- Configure Device E as the owner node for the subring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.
- Configure Device F as the neighbor node for the subring, GigabitEthernet 1/0/1 as ERPS ring member port 0 and the RPL port, and GigabitEthernet 1/0/2 as ERPS ring member port 1.

Figure 13 Network diagram



Procedure

2. Configure Device A.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceA] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceA-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
```

Configure the control VLAN.

```
[DeviceA-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

```
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

```
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
```

Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port.

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceA] erps enable
```

3. Configure Device B.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceB] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceB-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
```

Configure the control VLAN.

```
[DeviceB-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

```
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
```

Create track entry 3 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

```
[DeviceB] track 3 cfd cc service-instance 3 mep 3002
```

Associate GigabitEthernet 1/0/2 with track entry 3 and bring up the port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceB] erps enable
```

4. Configure Device C.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
```

```
[DeviceC-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
```

Create ERPS ring 1.

```
[DeviceC] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceC-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceC-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

```
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

```
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

Create ERPS ring 2.

```
[DeviceC] erps ring 2
```

Configure ERPS ring member ports.

```
[DeviceC-erps-ring2] port0 interface gigabitethernet 1/0/3
```

Configure ERPS ring 2 as the subring.

```
[DeviceC-erps-ring2] ring-type sub-ring
```

Create ERPS instance 1.

```
[DeviceC-erps-ring2] instance 1
```

Configure the node role.

```
[DeviceC-erps-ring2-inst1] node-role interconnection port0
```

Configure the control VLAN.

```
[DeviceC-erps-ring2-inst1] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceC-erps-ring2-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceC-erps-ring2-inst1] instance enable
[DeviceC-erps-ring2-inst1] quit
```

```
[DeviceC-erps-ring2] quit
```

Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.

```
[DeviceC] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5
```

Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/3.

```
[DeviceC] cfd meplist 5001 5002 service-instance 5
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] cfd mep 5001 service-instance 5 outbound
[DeviceC-GigabitEthernet1/0/3] cfd cc service-instance 5 mep 5001 enable
[DeviceC-GigabitEthernet1/0/3] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 3.

```
[DeviceC] track 1 cfd cc service-instance 5 mep 5001
```

Associate GigabitEthernet 1/0/3 with track entry 1 and bring up the port.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port erps ring 2 instance 1 track 1
[DeviceC-GigabitEthernet1/0/3] undo shutdown
[DeviceC-GigabitEthernet1/0/3] quit
```

Enable ERPS.

```
[DeviceC] erps enable
```

5. Configure Device D.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/3
```

```
[DeviceD-GigabitEthernet1/0/3] link-delay 0
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/3] quit
```

Create ERPS ring 1.

```
[DeviceD] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceD-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceD-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
[DeviceD-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

```
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

```
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

Create ERPS ring 2.

```
[DeviceD] erps ring 2
```

Configure ERPS ring member ports.

```
[DeviceD-erps-ring2] port0 interface gigabitethernet 1/0/3
```

Configure ERPS ring 2 as the subring.

```
[DeviceD-erps-ring2] ring-type sub-ring
```

Create ERPS instance 1.

```
[DeviceD-erps-ring2] instance 1
```

Configure the node role.

```
[DeviceD-erps-ring2-inst1] node-role interconnection port0
```

Configure the control VLAN.

```
[DeviceD-erps-ring2-inst1] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceD-erps-ring2-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceD-erps-ring2-inst1] instance enable
[DeviceD-erps-ring2-inst1] quit
[DeviceD-erps-ring2] quit
```

Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.

```
[DeviceD] cfd service-instance 6 ma-id vlan-based md MD_A vlan 6
```

Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6002 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/3.

```
[DeviceD] cfd meplist 6001 6002 service-instance 6
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 6002 service-instance 6 outbound
[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 6 mep 6002 enable
[DeviceD-GigabitEthernet1/0/3] quit
```

Create track entry 3 and associate it with the CC function of CFD for MEP 6002 in Ethernet service instance 6.

```
[DeviceD] track 3 cfd cc service-instance 6 mep 6002
```

Associate GigabitEthernet 1/0/3 with track entry 3 and bring up the port.

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] port erps ring 2 instance 1 track 3
[DeviceD-GigabitEthernet1/0/3] undo shutdown
[DeviceD-GigabitEthernet1/0/3] quit
```

Enable ERPS.

```
[DeviceD] erps enable
```

6. Configure Device E.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
```

Create ERPS ring 2.

```
[DeviceE] erps ring 2
```

Configure ERPS ring member ports.

```
[DeviceE-erps-ring2] port0 interface gigabitethernet 1/0/1
[DeviceE-erps-ring2] port1 interface gigabitethernet 1/0/2
```

Configure ERPS ring 2 as the subring.

```
[DeviceE-erps-ring2] ring-type sub-ring
```

Create ERPS instance 1.

```
[DeviceE-erps-ring2] instance 1
```

Configure the node role.

```
[DeviceE-erps-ring2] node-role owner rpl port0
```

Configure the control VLAN.

```
[DeviceE-erps-ring2-inst1] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceE-erps-ring2-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceE-erps-ring2-inst1] instance enable
[DeviceE-erps-ring2-inst1] quit
[DeviceE-erps-ring2] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceE] cfd enable
```

```
[DeviceE] cfd md MD_A level 5
```

Create Ethernet service instance 6, in which the MA is identified by a VLAN and serves VLAN 6.

```
[DeviceE] cfd service-instance 6 ma-id vlan-based md MD_A vlan 6
```

Configure a MEP list in Ethernet service instance 6, create outward-facing MEP 6001 in Ethernet service instance 6, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceE] cfd meplist 6001 6002 service-instance 6
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] cfd mep 6001 service-instance 6 outbound
[DeviceE-GigabitEthernet1/0/2] cfd cc service-instance 6 mep 6001 enable
[DeviceE-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.

```
[DeviceE] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7
```

Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7001 in Ethernet service instance 7, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceE] cfd meplist 7001 7002 service-instance 7
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd mep 7001 service-instance 7 outbound
[DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7001 enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 6001 in Ethernet service instance 6.

```
[DeviceE] track 1 cfd cc service-instance 6 mep 6001
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 7001 in Ethernet service instance 7.

```
[DeviceE] track 2 cfd cc service-instance 7 mep 7001
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceE] erps enable
```

7. Configure Device F.

Create VLANs 1 to 30, map these VLANs to MSTI 1, and activate the MST region configuration.

```
<DeviceF> system-view
[DeviceF] vlan 1 to 30
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1 to 30
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

Configure the port as a trunk port and assign it to VLANs 1 to 30.

```
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/2] quit
```

Create ERPS ring 2.

```
[DeviceF] erps ring 2
```

Configure ERPS ring member ports.

```
[DeviceF-erps-ring2] port0 interface gigabitethernet 1/0/1
[DeviceF-erps-ring2] port1 interface gigabitethernet 1/0/2
```

Configure ERPS ring 2 as the subring.

```
[DeviceF-erps-ring2] ring-type sub-ring
```

Create ERPS instance 1.

```
[DeviceF-erps-ring2] instance 1
```

Configure the node role.

```
[DeviceF-erps-ring2] node-role neighbor rpl port0
```

Configure the control VLAN.

```
[DeviceF-erps-ring2-inst1] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceF-erps-ring2-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceF-erps-ring2-inst1] instance enable
[DeviceF-erps-ring2-inst1] quit
[DeviceF-erps-ring2] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceF] cfd enable
[DeviceF] cfd md MD_A level 5
```

Create Ethernet service instance 5, in which the MA is identified by a VLAN and serves VLAN 5.

```
[DeviceF] cfd service-instance 5 ma-id vlan-based md MD_A vlan 5
```

Configure a MEP list in Ethernet service instance 5, create outward-facing MEP 5002 in Ethernet service instance 5, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceF] cfd meplist 5001 5002 service-instance 5
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] cfd mep 5002 service-instance 5 outbound
[DeviceF-GigabitEthernet1/0/2] cfd cc service-instance 5 mep 5002 enable
```

```
[DeviceF-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 7, in which the MA is identified by a VLAN and serves VLAN 7.

```
[DeviceF] cfd service-instance 7 ma-id vlan-based md MD_A vlan 7
```

Configure a MEP list in Ethernet service instance 7, create outward-facing MEP 7002 in Ethernet service instance 7, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceF] cfd meplist 7001 7002 service-instance 7
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] cfd mep 7002 service-instance 7 outbound
[DeviceF-GigabitEthernet1/0/1] cfd cc service-instance 7 mep 7002 enable
[DeviceF-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 5001 in Ethernet service instance 5.

```
[DeviceF] track 1 cfd cc service-instance 5 mep 5002
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] port erps ring 2 instance 1 track 1
[DeviceF-GigabitEthernet1/0/2] undo shutdown
[DeviceF-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 7002 in Ethernet service instance 7.

```
[DeviceF] track 2 cfd cc service-instance 7 mep 7002
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] port erps ring 2 instance 1 track 2
[DeviceF-GigabitEthernet1/0/1] undo shutdown
[DeviceF-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceF] erps enable
```

Verifying the configuration

Display information about ERPS instance 1 for Device A.

```
[Device A] display erps detail ring 1
 Ring ID               : 1
 Port0                 : GigabitEthernet1/0/1
 Port1                 : GigabitEthernet1/0/2
 Subring               : Yes
 Default MAC           : No
 Instance ID           : 1
 Node role             : Owner
 Node state            : Idle
 Connect(ring/instance): -
 Control VLAN          : 100
 Protected VLAN        : Reference-instance 1
 Guard timer           : 500 ms
 Hold-off timer        : 0 ms
 WTR timer             : 5 min
 Revertive operation   : Revertive
 Enable status         : Yes, Active status : Yes
```

```
R-APS level            : 7
Port                   PortRole                PortStatus
--------------------------------------------------------------------------------
Port0                  RPL                     Block
Port1                  Non-RPL                 Up
```

The output shows the following information:

- Device A is the owner node.
- The ERPS ring is in idle state.
- The RPL port is blocked.
- The non-RPL port is unblocked.

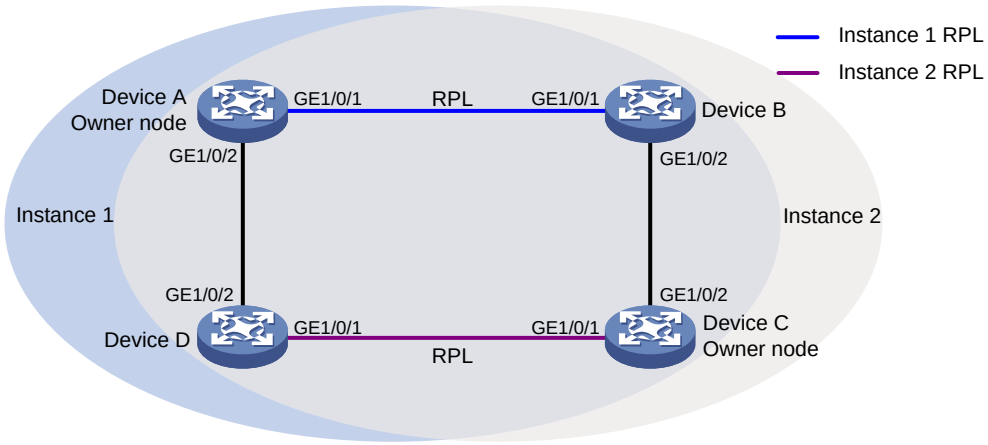
Example: Configuring one-ring multi-instance load balancing

Network configuration

As shown in Figure 14, perform the following tasks to improve network resource utilization and implement load balancing among links:

- Configure ERPS instances 1 and 2 on the ERPS ring.
- For ERPS instance 1, configure the following items:
  - Configure Device A as the owner node.
  - Configure the link between Devices A and Device B as the RPL.
  - Configure VLAN 100 as the control VLAN.
  - Configure VLANs 1 to 30 as the protected VLANs.
- For ERPS instance 2, configure the following items:
  - Configure Device A as the owner node.
  - Configure the link between Devices C and Device D as the RPL.
  - Configure VLAN 100 as the control VLAN.
  - Configure VLANs 31 to 60 as the protected VLANs.

Figure 14 Network diagram



Procedure

2. Configure Device A.

Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```
<DeviceA> system-view
[DeviceA] vlan 1 to 60
```

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
[DeviceA-mst-region] instance 2 vlan 31 to 60
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 60.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceA-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceA] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceA-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceA-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceA-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceA-erps-ring1-inst1] node-role owner rpl port0
```

Configure the control VLAN.

```
[DeviceA-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceA-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceA-erps-ring1-inst1] instance enable
[DeviceA-erps-ring1-inst1] quit
[DeviceA-erps-ring1] quit
```

Create ERPS instance 2.

```
[DeviceA-erps-ring1] instance 2
```

Configure the control VLAN.

```
[DeviceA-erps-ring1-inst2] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceA-erps-ring1-inst2] protected-vlan reference-instance 2
```

Enable ERPS for instance 2.

```
[DeviceA-erps-ring1-inst2] instance enable
[DeviceA-erps-ring1-inst2] quit
```

```
[DeviceA-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2001 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceA] cfd meplist 2001 2002 service-instance 2
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound
[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1001 in Ethernet service instance 1.

```
[DeviceA] track 1 cfd cc service-instance 1 mep 1001
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port for ERPS instances 1 and 2.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceA-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 2001 in Ethernet service instance 2.

```
[DeviceA] track 2 cfd cc service-instance 2 mep 2001
```

Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port for ERPS instances 1 and 2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceA-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceA] erps enable
```

3. Configure Device B.

Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```
<DeviceB> system-view
[DeviceB] vlan 1 to 60
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
[DeviceB-mst-region] instance 2 vlan 31 to 60
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 60.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceB-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceB] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceB-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceB-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceB-erps-ring1] instance 1
```

Configure the node role.

```
[DeviceB-erps-ring1-inst1] node-role neighbor rpl port0
```

Configure the control VLAN.

```
[DeviceB-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceB-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceB-erps-ring1-inst1] instance enable
[DeviceB-erps-ring1-inst1] quit
[DeviceB-erps-ring1] quit
```

Create ERPS instance 2.

```
[DeviceB-erps-ring1] instance 2
```

Configure the control VLAN.

```
[DeviceB-erps-ring1-inst2] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceB-erps-ring1-inst2] protected-vlan reference-instance 2
```

Enable ERPS for instance 2.

```
[DeviceB-erps-ring1-inst2] instance enable
[DeviceB-erps-ring1-inst2] quit
[DeviceB-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
```

Create Ethernet service instance 1, in which the MA is identified by a VLAN and serves VLAN 1.

```
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 1
```

Configure a MEP list in Ethernet service instance 1, create outward-facing MEP 1002 in Ethernet service instance 1, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceB] cfd meplist 1001 1002 service-instance 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound
[DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceB] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3002 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] cfd mep 3002 service-instance 3 outbound
[DeviceB-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3002 enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 1002 in Ethernet service instance 1.

```
[DeviceB] track 1 cfd cc service-instance 1 mep 1002
```

Associate GigabitEthernet 1/0/1 with track entry 1 and bring up the port for ERPS instances 1 and 2.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 1
[DeviceB-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 3002 in Ethernet service instance 3.

```
[DeviceB] track 2 cfd cc service-instance 3 mep 3002
```

Associate GigabitEthernet 1/0/2 with track entry 2 and bring up the port for ERPS instances 1 and 2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 2
[DeviceB-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

Enable ERPS.

```
[DeviceB] erps enable
```

4. Configure Device C.

Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```
<DeviceC> system-view
[DeviceC] vlan 1 to 60
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] instance 2 vlan 31 to 60
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 60.

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceC-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceC] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceC-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceC-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceC-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceC-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceC-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceC-erps-ring1-inst1] instance enable
[DeviceC-erps-ring1-inst1] quit
[DeviceC-erps-ring1] quit
```

Create ERPS instance 2.

```
[DeviceC-erps-ring1] instance 2
```

Configure the node role.

```
[DeviceC-erps-ring1-inst2] node-role owner rpl port0
```

Configure the control VLAN.

```
[DeviceC-erps-ring1-inst2] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceC-erps-ring1-inst2] protected-vlan reference-instance 2
```

Enable ERPS for instance 2.

```
[DeviceC-erps-ring1-inst2] instance enable
[DeviceC-erps-ring1-inst2] quit
[DeviceC-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceC] cfd enable
[DeviceC] cfd md MD_A level 5
```

Create Ethernet service instance 3, in which the MA is identified by a VLAN and serves VLAN 3.

```
[DeviceC] cfd service-instance 3 ma-id vlan-based md MD_A vlan 3
```

Configure a MEP list in Ethernet service instance 3, create outward-facing MEP 3001 in Ethernet service instance 3, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceC] cfd meplist 3001 3002 service-instance 3
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] cfd mep 3001 service-instance 3 outbound
[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 3 mep 3001 enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceC] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4001 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceC] cfd meplist 4001 4002 service-instance 4
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 outbound
[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 3001 in Ethernet service instance 3.

```
[DeviceC] track 1 cfd cc service-instance 3 mep 3001
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port for ERPS instances 1 and 2.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceC-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4001 in Ethernet service instance 4.

```
[DeviceC] track 2 cfd cc service-instance 4 mep 4001
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port for ERPS instances 1 and 2.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceC-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceC] erps enable
```

5. Configure Device D.

Create VLANs 1 to 60, map VLANs 1 to 30 to MSTI 1, map VLANs 31 to 60 to MSTI 2, and activate the MST region configuration.

```
<DeviceD> system-view
[DeviceD] vlan 1 to 60
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] instance 2 vlan 31 to 60
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Set the link state change suppression interval to 0 seconds on GigabitEthernet 1/0/1.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Configure the port as a trunk port and assign it to VLANs 1 to 60.

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 60
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 60
[DeviceD-GigabitEthernet1/0/2] quit
```

Create ERPS ring 1.

```
[DeviceD] erps ring 1
```

Configure ERPS ring member ports.

```
[DeviceD-erps-ring1] port0 interface gigabitethernet 1/0/1
[DeviceD-erps-ring1] port1 interface gigabitethernet 1/0/2
```

Create ERPS instance 1.

```
[DeviceD-erps-ring1] instance 1
```

Configure the control VLAN.

```
[DeviceD-erps-ring1-inst1] control-vlan 100
```

Configure the protected VLANs.

```
[DeviceD-erps-ring1-inst1] protected-vlan reference-instance 1
```

Enable ERPS for instance 1.

```
[DeviceD-erps-ring1-inst1] instance enable
[DeviceD-erps-ring1-inst1] quit
```

Create ERPS instance 2.

```
[DeviceD-erps-ring1] instance 2
```

Configure the node role.

```
[DeviceD-erps-ring1-inst2] node-role neighbor rpl port0
```

Configure the control VLAN.

```
[DeviceD-erps-ring1-inst2] control-vlan 110
```

Configure the protected VLANs.

```
[DeviceD-erps-ring1-inst2] protected-vlan reference-instance 2
```

Enable ERPS for instance 2.

```
[DeviceD-erps-ring1-inst2] instance enable
[DeviceD-erps-ring1-inst2] quit
[DeviceD-erps-ring1] quit
```

Enable CFD, and create a level-5 MD named **MD_A**.

```
[DeviceD] cfd enable
[DeviceD] cfd md MD_A level 5
```

Create Ethernet service instance 2, in which the MA is identified by a VLAN and serves VLAN 2.

```
[DeviceD] cfd service-instance 2 ma-id vlan-based md MD_A vlan 2
```

Configure a MEP list in Ethernet service instance 2, create outward-facing MEP 2002 in Ethernet service instance 2, and enable CCM sending on GigabitEthernet 1/0/2.

```
[DeviceD] cfd meplist 2001 2002 service-instance 2
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Create Ethernet service instance 4, in which the MA is identified by a VLAN and serves VLAN 4.

```
[DeviceD] cfd service-instance 4 ma-id vlan-based md MD_A vlan 4
```

Configure a MEP list in Ethernet service instance 4, create outward-facing MEP 4002 in Ethernet service instance 4, and enable CCM sending on GigabitEthernet 1/0/1.

```
[DeviceD] cfd meplist 4001 4002 service-instance 4
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4002 service-instance 4 outbound
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4002 enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Create track entry 1 and associate it with the CC function of CFD for MEP 2002 in Ethernet service instance 2.

```
[DeviceD] track 1 cfd cc service-instance 2 mep 2002
```

Associate GigabitEthernet 1/0/2 with track entry 1 and bring up the port for ERPS instances 1 and 2.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 1 track 1
[DeviceD-GigabitEthernet1/0/2] port erps ring 1 instance 2 track 1
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

Create track entry 2 and associate it with the CC function of CFD for MEP 4002 in Ethernet service instance 4.

```
[DeviceD] track 2 cfd cc service-instance 4 mep 4002
```

Associate GigabitEthernet 1/0/1 with track entry 2 and bring up the port for ERPS instances 1 and 2.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 2
[DeviceD-GigabitEthernet1/0/1] port erps ring 1 instance 2 track 2
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

Enable ERPS.

```
[DeviceD] erps enable
```

Verifying the configuration

Display information about ERPS instance 1 for Device A.

```
[Device A] display erps detail ring 1
 Ring ID               : 1
 Port0                 : GigabitEthernet1/0/1
 Port1                 : GigabitEthernet1/0/2
 Subring               : No
 Default MAC           : No
 Instance ID           : 1
 Node role             : Owner
 Node state            : Idle
 Connect(ring/instance): -
 Control VLAN          : 100
 Protected VLAN        : Reference-instance 1
 Guard timer           : 500 ms
 Hold-off timer        : 0 ms
 WTR timer             : 5 min
 Revertive operation   : Revertive
 Enable status         : Yes, Active status : Yes
 R-APS level           : 7
 Port                  PortRole               PortStatus
 --------------------------------------------------------------------------------
 Port0                 RPL                    Block
 Port1                 Non-RPL                Up

 Instance ID           : 2
 Node role             : Normal
 Node state            : Idle
 Connect(ring/instance): -
 Control VLAN          : 100
 Protected VLAN        : Reference-instance 2
 Guard timer           : 500 ms
 Hold-off timer        : 0 ms
 WTR timer             : 5 min
 Revertive operation   : Revertive
 Enable status         : Yes, Active status : Yes
 R-APS level           : 7
 Port                  PortRole               PortStatus
 --------------------------------------------------------------------------------
 Port0                 Non-RPL                Up
 Port1                 Non-RPL                Up
```

The output shows the following information:

- For ERPS instance 1:
  - Device A is the owner node.
  - The ERPS ring is in idle state.

    - The RPL port is blocked.
    - The non-RPL port is unblocked.
- For ERPS instance 2:
    - Device A is a normal node.
    - The ERPS ring is in idle state.
    - The non-RPL port is unblocked.

Troubleshooting ERPS

The owner node cannot receive SF packets from a faulty node when the link state is normal

Symptom

The link between the owner node and the faulty node is available, but the owner node cannot receive SF packets sent by the faulty node. The RPL port is blocked.

Analysis

Possible reasons include:

- ERPS is not enabled for some nodes on the ERPS ring.
- The ring IDs are different for the nodes on the same ERPS ring.
- The control VLAN IDs are different for the nodes in the same ERPS instance.
- A port on the ERPS ring is faulty.

Solutions

To resolve the problem:

- Use the **display erps** command to examine whether ERPS is enabled for all nodes on the ERPS ring. If ERPS is disabled for some nodes, use the **erps enable** command to enable ERPS for the nodes.
- Set the same ring ID for all nodes on a ERPS ring and configure the same control VLAN for all nodes in an ERPS instance.
- Use the **display erps detail** command to examine the port status for all nodes. Bring up the ports in down state.
- Use the **debugging erps** command on all nodes to view debugging information about packets and node status.

Command reference

control-vlan

Use **control-vlan** to configure the control VLAN for an ERPS instance.

Use **undo control-vlan** to restore the default.

Syntax

control-vlan *vlan-id*

undo control-vlan

Default

An ERPS instance does not have control VLANs.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the ID of the control VLAN, in the range of 2 to 4094.

Examples

Configure VLAN 100 as the control VLAN for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] control-vlan 100
```

Related commands

instance

display erps

Use **display erps** to display brief ERPS ring information.

Syntax

display erps

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief ERPS ring information.

```
<Sysname> display erps
ERPS protocol status: Enabled
ERPS tcn-propagation: Enabled
Flags: R -- RPL, F -- Faulty, B -- Blocked,
       FS -- Forced switch, MS -- Manual switch
Ring   Instance   NodeRole   NodeState    Port0     Port1    Status
--------------------------------------------------------------------------
1      1          Owner      Idle         R,B               Enabled
1      2          Normal     Idle                           Disabled
2      1          Owner      Idle         R,B               Enabled
2      2          Normal     Idle                           Disabled
```

Table 3 Command output

Field	Description
ERPS protocol status	ERPS state: • **Enabled**—Globally enabled. • **Disabled**—Globally disabled.
ERPS tcn-propagation	State of the flush packet transparent transmission feature: • **Enabled**—Globally enabled.

Field	Description
	• **Disabled**—Globally disabled.
Ring	ERPS ring ID.
Instance	ERPS instance ID.
NodeRole	Node type: • Owner. • Neighbor. • Interconnection. • Normal.
NodeState	Node state: • **Idle**—The ERPS ring enters the idle state after initialization. • **Protection**—The ERPS ring enters the protection state when a link fails. • **MS**—Manual switching mode. • **FS**—Forced switching mode. • **Pending**—Transient mode between any two states. • **-**—ERPS is disabled for the ERPS instance or disabled globally.
Port0	State of port 0: • **R**—The port is an RPL port. • **B**—The port is blocked. • **F**—The port is unavailable and the link for the port is faulty. • **FS**—The port is in FS mode. • **MS**—The port is in MS mode. • **-**—The port is not an ERPS ring member port. If this field is blank, the port is not in any of the previous states.
Port1	State of port 1: • **R**—The port is an RPL port. • **B**—The port is blocked. • **F**—The port is unavailable and the link for the port is faulty. • **FS**—The port is in FS mode. • **MS**—The port is in MS mode. • **-**—The port is not an ERPS ring member port. If this field is blank, the port is not in any of the previous states.
Status	State of the ERPS instance: • Enabled. • Disabled.

display erps detail

Use **display erps detail** to display detailed ERPS ring information.

Syntax

display erps detail ring *ring-id* [**instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays detailed information about all instances for the ERPS ring.

Examples

Display detailed information about instance 1 of ERPS ring 1.

```
<Sysname> display erps detail ring 1 instance 1
Ring ID                : 1
Port0                  : GigabitEthernet1/0/1
Port1                  : GigabitEthernet1/0/2
Subring                : Yes
Default MAC            : Yes

Instance ID            : 1
Node role              : Owner
Node state             : Idle
Connect (ring/instance): (1/2), (2/3)
Control VLAN           : 100
Protected VLAN         : Reference-instance 0 to 2
Guard timer            : 500 ms
Hold-off timer         : 1 sec
WTR timer              : 5 min
Revertive operation    : Non-revertive
Enable status          : Yes, Active Status : Yes
R-APS level            : 1
Port                   PortRole               PortStatus
--------------------------------------------------------------------
Port0                  RPL                    Block
Port1                  Non-RPL                Up
```

Display detailed information about all instances of ERPS ring 1.

```
<Sysname> display erps detail ring 1
Ring ID               : 1
Port0                 : GigabitEthernet1/0/1
Port1                 : GigabitEthernet1/0/2
Subring               : Yes
Default MAC           : Yes

Instance ID           : 1
Node role             : Owner
Node state            : Idle
Connect(ring/instance): (1/2), (2/3)
Control VLAN          : 100
Protected VLAN        : Reference-instance 0 to 2
Guard timer           : 500 ms
Hold-off timer        : 1 sec
```

```
WTR timer             : 5 min
Revertive operation   : Non-revertive
Enable status         : Yes, Active Status : Yes
R-APS level           : 1
Port                  PortRole              PortStatus
--------------------------------------------------------------------------
Port0                 RPL                   Block
Port1                 Non-RPL               Up

Instance ID           : 2
Node role             : Neighbor
Node state            : Idle
Connect(ring/instance): (1/2), (2/3)
Control VLAN          : 200
Protected VLAN        : Reference-instance 3
Guard timer           : 500 ms
Hold-off timer        : 1 sec
Wtr timer             : 5 min
Revertive operation   : Non-revertive
Enable status         : Yes, Active Status : Yes
R-APS level           : 1
Port                  PortRole              PortStatus
--------------------------------------------------------------------------
Port0                 RPL                   Block
Port1                 Non-RPL               Up
```

Table 4 Command output

Field	Description
Port0	ERPS ring member port 0.
Port1	ERPS ring member port 1.
Subring	ERPS subring status: • **Yes**—The ring is a subring. • **No**—The ring is not a subring.
Default MAC	Default MAC address status: • **Yes**—The last byte is 1 in the destination MAC address of R-APS packets. • **No**—The last byte is the ring ID in the destination MAC address of R-APS packets.
Node role	Node type: • Owner. • Neighbor. • Interconnection. • Normal.
Node state	Node state: • **Idle**—The ERPS ring enters the idle status after initialization. • **Protection**—The ERPS ring enters the protection state when a link fails. • **MS**—Manual switching mode.

Field	Description
	• **FS**—Forced switching mode. • **Pending**—Transient mode between any two states. • **-**—ERPS is disabled for the ERPS instance or disabled globally.
Connect(ring/instance)	Ring or instance associated with the ERPS instance.
Control VLAN	Control VLAN of the ERPS instance.
Protected VLAN	List of VLANs protected by the ERPS instance, which are represented by MSTIs. To view the mapping between MSTIs and VLANs, use the **display stp region-configuration** command.
Guard timer	Guard timer in milliseconds.
Hold-off timer	Hold-off timer in milliseconds.
WTR timer	WTR timer in minutes.
Revertive operation	Revertive mode: • Non-revertive. • Revertive.
Enable status	ERPS status for the instance: • **Yes**—Enabled. • **No**—Disabled.
Active Status	Global ERPS status and ERPS status for the instance: • **Yes**—Enabled. • **No**—Disabled.
R-APS level	Level of the R-APS packets.
Port	ERPS ring member port.
PortRole	Port role: • **RPL**—The port is an RPL port. • **Non-RPL**—The port is not an RPL port.
Port Status	Port status: • **Block**—The port is blocked. • **Up**—The link is up. • **Down**—The link is down.

display erps statistics

Use **display erps statistics** to display ERPS packet statistics.

Syntax

display erps statistics *ring-id* [**instance** *instance-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command displays packet statistics for all instances of the ERPS ring.

Examples

Display packet statistics for all instances of ERPS ring 1.

```
<Sysname> display erps statistics ring 1
  Statistics for ERPS ring 1 instance 1:
  R-APS      Port0(Tx/Rx)             Port1(Tx/Rx)
  ------------------------------------------------------
  NR         1/1                      1/1
  NR,RB      0/1                      0/1
  SF         1/0                      1/0
  MS         0/0                      0/0
  FS         0/0                      0/0
  Total      2/2                      2/2

  Statistics for ERPS ring 1 instance 2:
  R-APS      Port0(Tx/Rx)             Port1(Tx/Rx)
  ------------------------------------------------------
  NR         1/1                      1/1
  NR,RB      0/1                      0/1
  SF         1/0                      1/0
  MS         0/0                      0/0
  FS         0/0                      0/0
  Total      2/2                      2/2
```

Table 5 Command output

Field	Description
R-APS	Packet type.
Port0(Tx/Rx)	Packet statistics for port 0: • **Tx**—Transmitted packets. • **Rx**—Received packets.
Port1(Tx/Rx)	Packet statistics for port 1: • **Tx**—Transmitted packets. • **Rx**—Received packets.

erps clear

Use **erps clear** to remove the MS mode and FS mode settings for an ERPS ring.

Syntax

erps clear *ring-id* **instance** *instance-id*

Views

System view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

After you configure this command, the owner node can ignore the WTR timer and immediately switch traffic to the recovered link upon link recovery.

This command also switches an ERPS ring in non-revertive mode to revertive mode.

Examples

Remove the MS mode and FS mode settings for instance 1 on ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps clear ring 1 instance 1
```

erps enable

Use **erps enable** to enable ERPS globally.

Use **undo erps enable** to restore the default.

Syntax

erps enable

undo erps enable

Default

ERPS is disabled globally.

Views

System view

Predefined user roles

network-admin

Examples

Enable ERPS.

```
<Sysname> system-view
[Sysname] erps enable
```

erps ring

Use **erps ring** to create an ERPS ring.

Use **undo erps ring** to delete an ERPS ring.

Syntax

erps ring *ring-id*

undo erps ring *ring-id*

Default

No ERPS rings exist.

Views

System view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

Usage guideline

To delete an ERPS ring successfully, delete all ERPS instances on the ring first.

Examples

Create ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1]
```

Related commands

instance

erps switch

Use **erps switch** to configure the switching mode for an ERPS ring.

Syntax

erps switch { **force** | **manual** } **ring** *ring-id* **instance** *instance-id* { **port0** | **port1** }

Views

System view

Predefined user roles

network-admin

Parameters

force: Configures the forced switching mode.

manual: Configures the manual switching mode.

port0: Specifies the ERPS ring member port 0.

port1: Specifies the ERPS ring member port 1.

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

Configure the forced switching mode for port 1 of instance 1 on ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps switch force ring 1 instance 1 port0
```

erps tcn-propagation

Use **erps tcn-propagation** to enable flush packet transparent transmission for an interconnection node.

Use **undo erps tcn-propagation** to restore the default.

Syntax

erps tcn-propagation

undo erps tcn-propagation

Default

Flush packet transparent transmission is disabled for an interconnection node.

Views

System view

Predefined user roles

network-admin

Usage guideline

This command must be used together with the **sub-ring connect** command.

Examples

Enable flush packet transparent transmission for the interconnection node.

```
<Sysname> system-view
[Sysname] erps tcn-propagation
```

Related commands

sub-ring connect

instance

Use **instance** to create an instance for an ERPS ring.

Use **undo instance** to delete an instance from an ERPS ring.

Syntax

instance *instance-id*

undo instance *instance-id*

Default

An ERPS ring does not have instances.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Usage guidelines

You can create multiple instances for an ERPS ring. Each instance has its own protected VLAN, control VLAN, and RPL owner. Each instance maintains its own state machine and data. You can locate an ERPS instance by its ring ID and VLAN ID.

Examples

Create instance 1 for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1]
```

Related commands

erps ring

instance enable

Use **instance enable** to enable ERPS for an ERPS instance.

Use **undo instance enable** to disable ERPS for an ERPS instance.

Syntax

instance enable

undo instance enable

Default

ERPS is disabled for ERPS instances.

Views

ERPS instance view

Predefined user roles

network-admin

Examples

Create ERPS instance 1 and enable ERPS for the instance.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] control-vlan 100
[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2
[Sysname-erps-ring1-inst1] instance enable
```

Related commands

instance

node-role

Use **node-role** to configure the role for an ERPS node.

Use **undo node-role** to restore the default.

Syntax

node-role { { **owner** | **neighbor** } **rpl** | **interconnection** } { **port0** | **port1** }

undo node-role

Default

An ERPS node is a normal node.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

owner: Configures the owner node.

neighbor: Configures the neighbor node.

interconnection: Configures the interconnection node for connecting the major ring and subring.

Usage guidelines

You can configure an interconnection node only for a subring.

Examples

Configure instance 1 of ERPS ring 1 as an RPL owner node and configure port 0 as an RPL port.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] node-role owner rpl port0
```

port erps track

Use **port erps track** to associate an ERPS ring member port with a track entry.

Use **undo port erps track** to remove the association between an ERPS ring member port and a track entry.

Syntax

port erps ring *ring-id* **instance** *instance-id* **track** *track-entry-index*

undo port erps ring *ring-id* **instance** *instance-id* **track**

Default

An ERPS ring member port is not associated with track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

track-entry-index: Specifies a track entry by its ID in the range of 1 to 1024. For more information about specifying the track entry ID, see the **track cfd** command in "Track commands."

Usage guidelines

An ERPS ring member port collaborates with link detection protocols through track entries. ERPS supports only the CC feature of CFD to implement link detection.

Examples

Associate a track entry with GigabitEthernet 1/0/1 on the RPL owner node in instance 1 of ERPS ring 1.

```
<Sysname> system-view
```

```
[Sysname] erps ring 1
[Sysname-erps-ring1] port0 interface gigabitethernet 1/0/1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] node-role owner rpl port0
[Sysname-erps-ring1-inst1] quit
[Sysname-erps-ring1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port erps ring 1 instance 1 track 3
```

Related commands

track cfd

port0

Use **port0** to specify the first member port for an ERPS ring.

Use **undo port0** to restore the default.

Syntax

port0 interface *interface-type interface-number*

undo port0

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Examples

Specify GigabitEthernet 1/0/1 as the first member port for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] port0 interface gigabitethernet 1/0/1
```

port1

Use **port1** to specify the second member port for an ERPS ring.

Use **undo port1** to restore the default.

Syntax

port1 interface *interface-type interface-number*

undo port1

Default

No member ports exist in an ERPS ring.

Views

ERPS ring view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet interface or a Layer 2 aggregate interface by its type and number.

Examples

Specify GigabitEthernet 1/0/2 as the second member port for ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] port1 interface gigabitethernet 1/0/2
```

protected-vlan

Use **protected-vlan** to configure protected VLANs for an ERPS instance.

Use **undo protected-vlan** to delete protected VLANs for an ERPS instance.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLANs exist in an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

instance-id-list: Specifies a space-separated list of up to 10 MSTI items. Each item specifies an MSTI or a range of MSTIs in the form of *instance-id1* **to** *instance-id2*. The value for *instance-id2* must be greater than or equal to the value for *instance-id1*. The value range for the *instance-id* argument is 0 to 4094. The value 0 indicates CIST. You can use the **display stp region-configuration** command to display the VLAN-to-instance mappings. In PVST mode, the system automatically maps VLANs to MSTIs.

Usage guidelines

If you do not specify the **reference-instance** *instance-id-list* option, the **undo protected-vlan** command deletes all mappings between MSTIs and VLANs in the ERPS instance. The protected VLANs change if the mappings between the MSTIs and VLANs change.

Examples

Configure the protected VLANs for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] protected-vlan reference-instance 0 1 2
```

Related commands

display stp region-configuration

r-aps level

Use **r-aps level** to configure the level for R-APS packets.

Use **undo r-aps level** to restore the default.

Syntax

r-aps level *level-value*

undo r-aps level

Default

The R-APS packet level is 7.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

level-value: Specifies the R-APS packet level in the range of 0 to 7.

Usage guidelines

The R-APS packet level must be the same for all nodes in an instance of an ERPS ring.

Examples

Configure the R-APS packet level as 1 for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] r-aps level 1
```

r-aps ring-mac

Use **r-aps ring-mac** to configure the ring ID as the last byte of the destination MAC address for R-APS packets.

Use **undo r-aps ring-mac** to restore the default.

Syntax

r-aps ring-mac

undo r-aps ring-mac

Default

The last byte of the destination MAC address is 1 for the R-APS packets.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

Configure the ID of ERPS ring 2 as the last byte of the destination MAC address for R-APS packets.

```
<Sysname> system-view
[Sysname] erps ring 2
[Sysname-erps-ring2] r-aps ring-mac
```

reset erps statistics

Use **reset erps statistics** to clear ERPS packet statistics.

Syntax

reset erps statistics ring *ring-id* [**instance** *instance-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64. If you do not specify this option, this command clears packet statistics for all instances of the ERPS ring.

Examples

Clear packet statistics for instance 1 of ERPS ring 1.

```
<Sysname> reset erps statistics ring 1 instance 1
```

Related commands

display erps statistics

revertive-operation

Use **revertive-operation non-revertive** to set the non-revertive mode for an ERPS ring.

Use **undo revertive-operation** to restore the default.

Syntax

revertive-operation non-revertive

undo revertive-operation

Default

An ERPS ring operates in revertive mode.

Views

ERPS instance view

Predefined user roles

network-admin

Usage guidelines

In non-revertive mode, an owner node does not perform any operations when receiving NR packets. You can use the **erps clear** command to restore the revertive mode.

Examples

Set the non-revertive mode for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] revertive-operation non-revertive
```

ring-type sub-ring

Use **ring-type sub-ring** to configure the ERPS ring as a subring.

Use **undo ring-type sub-ring** to restore the default.

Syntax

ring-type sub-ring

undo ring-type

Default

An ERPS ring is a major ring.

Views

ERPS ring view

Predefined user roles

network-admin

Examples

Configure ERPS ring 1 as a subring.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] ring-type sub-ring
```

sub-ring connect

Use **sub-ring connect** to associate the subring with an ERPS ring.

Use **undo sub-ring connect** to remove the association.

Syntax

sub-ring connect ring *ring-id* **instance** *instance-id*

undo sub-ring connect ring *ring-id* **instance** *instance-id*

Default

A subring is not associated with ERPS rings.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

ring *ring-id*: Specifies an ERPS ring by its ID in the range of 1 to 255.

instance *instance-id*: Specifies an ERPS instance by its ID in the range of 1 to 64.

Examples

Configure ERPS ring 1 as a subring for instance 1, and associate the subring with ERPS ring 2.

```
<Sysname> system-view
[Sysname] erps ring 2
[Sysname-erps-ring2] instance 1
[Sysname-erps-ring2] quit
[Sysname] erps ring 1
[Sysname-erps-ring1] ring-type sub-ring
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] sub-ring connect ring 2 instance 1
```

Related commands

ring-type sub-ring

timer guard

Use **timer guard** to set the guard timer for an ERPS instance.

Use **undo timer guard** to restore the default.

Syntax

timer guard *guard-value*

undo timer guard

Default

The guard timer is 500 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

guard-value: Specifies the guard timer in the range of 0 to 2000 milliseconds and in step of 10.

Usage guidelines

The guard timer starts when the link recovers. The system processes only the flush packets before the guard timer expires. The guard timer prevents SF messages from impacting the network.

Examples

Set the guard timer to 30 milliseconds for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer guard 30
```

timer hold-off

Use **timer hold-off** to set the hold-off timer for an ERPS instance.

Use **undo timer hold-off** to restore the default.

Syntax

timer hold-off *hold-off-value*

undo timer hold-off

Default

The hold-off timer is 0 milliseconds for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

hold-off-value: Specifies the hold-off timer in the range of 0 to 10000 milliseconds and in step of 100.

Usage guidelines

The hold-off timer starts when the port detects a link fault. If the link fault persists when the hold-off timer expires, the port reports the link fault. The hold-off timer delays the fault report time and might impact the link recovery performance.

Examples

Set the hold-off timer to 300 milliseconds for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer hold-off 300
```

timer wtr

Use **timer wtr** to set the WTR timer for an ERPS instance.

Use **undo timer wtr** to restore the default.

Syntax

timer wtr *wtr-value*

undo timer wtr

Default

The WTR timer is 5 minutes for an ERPS instance.

Views

ERPS instance view

Predefined user roles

network-admin

Parameters

wtr-value: Specifies the WTR timer in the range of 1 to 12 minutes and in step of 1.

Usage guidelines

This timer prevents intermittent link failures from impacting the network.

Examples

Set the WTR timer to 3 minutes for instance 1 of ERPS ring 1.

```
<Sysname> system-view
[Sysname] erps ring 1
[Sysname-erps-ring1] instance 1
[Sysname-erps-ring1-inst1] timer wtr 3
```

Modified feature: Physical type of a combo interface

Feature change description

In this version and later, the **combo enable auto** command is supported, which configures a combo interface to autonegotiate its physical type.

Command changes

combo enable

Old syntax

combo enable { **copper** | **fiber** }

New syntax

combo enable { auto | copper | fiber }

Views

Ethernet interface view

Parameters

auto: Specifies the combo interface to autonegotiate its physical type.

Usage guidelines

When a combo interface acts as an IRF physical interface, you must manually configure the physical type of the combo interface as **copper** or **fiber**.

A combo interface in **auto** mode does not support the **duplex half**, **speed 10**, or **speed 100** command.

Change description

Before modification:

By default, the copper combo port is activated. You can specify the **copper** or **fiber** keyword to activate the copper or fiber combo port as needed.

After modification:

By default, a combo interface autonegotiates its physical type. When a combo autonegotiates its physical type, the actual physical type depends on the connected media:

- When the copper combo port is not connected to a twisted-pair cable and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
- When the copper combo port is connected to a twisted-pair cable and is up:
  a. If you install a transceiver module in the fiber combo port, the copper combo port is still activated before the device is rebooted.
  b. After the device is rebooted, the fiber combo port is activated.

- When the copper combo port is connected to a twisted-pair cable and is down and the fiber combo port has a transceiver module installed, the fiber combo port is activated.
- When the fiber combo port has a transceiver module installed, the fiber combo port is activated even if you connect a twisted-pair cable to the copper combo port.

If you need to specify the physical type of a physical interface according to the network requirements, you can specify the **copper** or **fiber** keyword to activate the copper or fiber combo port.

Release 3208P12

This release has the following changes:

New feature: PD detection mode

Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation

New feature: PD detection mode

Configuring the PD detection mode

About PD detection modes

The device detects PDs in one of the following modes:

- **None**—The device supplies power to PDs that are correctly connected to the device without causing short circuit.
- **Simple**—The device supplies power to PDs that comply with basic requirements of 802.3af or 802.3at.
- **Strict**—The device supplies power to PDs that comply with all requirements of 802.3af or 802.3at.

Restrictions and guidelines

Only PSEs with model LSP7POEB and LSP7POED support this configuration. To obtain your PSE model, see the **PSE Model** field in the output from the **`display poe pse`** command.

For this feature to take effect on nonstandard PDs, you must enable detection for nonstandard PDs by using the **`poe legacy enable`** command.

Procedure

1. Enter system view.

   `system-view`
2. Enter PI view.

   `interface` *`interface-type interface-number`*
3. Configure the PD detection mode.

   `poe detection-mode` { **`none`** | **`simple`** | **`strict`** }

   By default, the PD detection mode is strict.

Command reference

poe detection-mode

Use **`poe detection-mode`** to configure the PD detection mode.

Use **`undo poe detection-mode`** to restore the default.

Syntax

`poe detection-mode` { **`none`** | **`simple`** | **`strict`** }

`undo poe detection-mode`

Default

The PD detection mode is strict.

Views

PI view

Predefined user roles

network-admin

Parameters

none: Enables the device to supply power to PDs that are correctly connected to the device without causing short circuit.

simple: Enables the device to supply power to PDs that comply with basic requirements of 802.3af or 802.3at.

strict: Enables the device to supply power to PDs that comply with all requirements of 802.3af or 802.3at.

Usage guidelines

To configure the detection mode for nonstandard PDs, first execute the **poe legacy enable** command to enable detection for nonstandard PDs.

Examples

Configure the simple detection mode for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe detection-mode simple
```

Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation

Feature change description

In the ping operation, the value range for the length of ICMP or ICMPv6 echo requests was changed from 20 to 8100 bytes to 20 to 9600 bytes.

Command changes

Modified command: ping

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host*

Views

Any view

Parameters

-s *packet-size*: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range is 20 to 9600, and the default is 56.

Change description

Before modification: The value range for the *packet-size* argument is 20 to 8100 bytes.

After modification: The value range for the *packet-size* argument is 20 to 9600 bytes.

Modified command: ping ipv6

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-tc** *traffic-class* | **-v**] * *host*

Views

Any view

Parameters

-s *packet-size*: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range is 20 to 9600, and the default is 56.

Change description

Before modification: The value range for the *packet-size* argument is 20 to 8100 bytes.

After modification: The value range for the *packet-size* argument is 20 to 9600 bytes.

Release 3208P10

This release has the following changes:

- New feature: Automatic obtaining of the login username for temporary user role authorization
- New feature: 802.1X EAP-TLS fragmentation for packets sent to the server
- New feature: Enabling interface consistency check for ARP and MAC address entries
- New feature: 802.1X offline detection
- New feature: Enabling SAVI and setting the entry deletion delay by using commands
- Modified feature: Configuring MAC-based MAC authentication user accounts
- Modified feature: Port security NTK feature

New feature: Automatic obtaining of the login username for temporary user role authorization

Automatically obtaining the login username for temporary user role authorization

About automatic obtaining of the login username for temporary user role authorization

This feature is applicable only to the login from a user line that uses scheme authentication, which requires a username for login. This feature enables the device to automatically obtain the login username when the login user requests a temporary user role authorization from a remote authentication server.

Restrictions and guidelines

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This feature does not take effect on local password authentication for temporary user role authorization.

Procedure

1. Enter system view.

   `system-view`

2. Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

   `super use-login-username`

   By default, the device requests a username at the prompt when a login user requests temporary user role authorization from a remote authentication server.

Command reference

super use-login-username

Use **super use-login-username** to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use **undo super use-login-username** to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device requests a username at the prompt when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

```
<Sysname> system-view
[Sysname] super use-login-username
```

New feature: 802.1X EAP-TLS fragmentation for packets sent to the server

Setting the maximum length of an EAP-TLS fragment sent to the server

About setting the maximum length of an EAP-TLS fragment sent to the server

Some RADIUS servers cannot process oversized packets. If the length of a RADIUS packet exceeds the maximum packet length allowed by the servers, the client will fail the authentication.

The device might send oversized packets to such a RADIUS server when it uses the EAP relay mode and the EAP-TLS authentication method in remote authentication. The device encapsulates

the EAP-TLS messages received from a client into the EAP-Message attribute of the RADIUS packets that will be sent to the server.

To avoid authentication failures caused by oversized packets, you can fragment the EAP-TLS messages that will be sent to the server in RADIUS packets.

Set a proper maximum length for the EAP-TLS fragments according to the maximum packet length allowed by the server.

After receiving all EAP-TLS fragments, the server will reassemble the EAP-TLS fragments and obtain the complete authentication information of the client.

For example, the maximum packet length allowed by the server is 1200 bytes and the length of a RADIUS packet (excluding the EAP-Message attribute) is 800 bytes. To make sure the maximum length of a RADIUS packet does not exceed 1200 bytes, you must set the maximum length of an EAP-TLS fragment to a value less than 400 bytes.

Restrictions and guidelines

For 802.1X EAP-TLS fragmentation and the maximum fragment length to take effect, you must set the EAP message handling method to EAP relay.

Procedure

1. Enter system view.

   system-view

2. Set the maximum length of an EAP-TLS fragment that will be sent in an authentication packet to the server.

   dot1x eap-tls-fragment to-server *eap-tls-max-length*

   By default, EAP-TLS messages are not fragmented by 802.1X EAP-TLS fragmentation.

Command reference

dot1x eap-tls-fragment to-server

Use **dot1x eap-tls-fragment to-server** to set the maximum length of an EAP-TLS fragment that will be sent in an authentication packet to the server.

Use **undo dot1x eap-tls-fragment to-server** to restore the default.

Syntax

dot1x eap-tls-fragment to-server *eap-tls-max-length*

undo dot1x eap-tls-fragment to-server

Default

EAP-TLS messages are not fragmented by 802.1X EAP-TLS fragmentation.

Views

System view

Predefined user roles

network-admin

Parameters

eap-tls-max-length: Sets the maximum length of an EAP-TLS fragment in bytes. The value range is 100 to 1500.

Usage guidelines

IMPORTANT:

For this command to take effect, you must set the EAP message handling method to EAP relay.

Some RADIUS servers cannot process oversized packets. If the length of a RADIUS packet exceeds the maximum packet length allowed by the servers, the client will fail the authentication.

The device might send oversized packets to such a RADIUS server when it uses the EAP relay mode and the EAP-TLS authentication method in remote authentication. The device encapsulates the EAP-TLS messages received from a client into the EAP-Message attribute of the RADIUS packets that will be sent to the server.

To avoid authentication failures caused by oversized packets, you can fragment the EAP-TLS messages that will be sent to the server in RADIUS packets.

Use this command to set a proper maximum length for the EAP-TLS fragments according to the maximum packet length allowed by the server.

After receiving all EAP-TLS fragments, the server will reassemble the EAP-TLS fragments and obtain the complete authentication information of the client.

For example, the maximum packet length allowed by the server is 1200 bytes and the length of a RADIUS packet (excluding the EAP-Message attribute) is 800 bytes. To make sure the maximum length of a RADIUS packet does not exceed 1200 bytes, you must set the maximum length of an EAP-TLS fragment to a value less than 400 bytes.

Examples

Set the maximum length to 400 bytes for the EAP-TLS fragments that will be sent in packets to the server.

```
<Sysname> system-view
[Sysname] dot1x eap-tls-fragment to-server 400
```

Related commands

dot1x authentication-method

New feature: Enabling interface consistency check for ARP and MAC address entries

Enabling interface consistency check for ARP and MAC address entries

About interface consistency check for ARP and MAC address entries

In an instable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency for the ARP and MAC address entry of a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Procedure

1. Enter system view.

   system-view

2. Enabling interface consistency check for ARP and MAC address entries.

arp mac-interface-consistency check enable

By default, enabling interface consistency check for ARP and MAC address entries is disabled.

Command reference

arp mac-interface-consistency check enable

Use **arp mac-interface-consistency check enable** to enable interface consistency check for ARP and MAC address entries.

Use **undo arp mac-interface-consistency check enable** to disable this feature.

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

Default

Enabling interface consistency check for ARP and MAC address entries is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In an instable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency for the ARP and MAC address entry of a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Use **display mac-address** to display MAC address entries.

Examples

Enable interface consistency check for ARP and MAC address entries.

```
<Sysname> system-view
[Sysname] arp mac-interface-consistency check enable
```

Related commands

display mac-address (*Layer 2—LAN Switching Command Reference*)

New feature: 802.1X offline detection

Configuring 802.1X offline detection

About 802.1X offline detection

The 802.1X offline detection feature monitors the online status of 802.1X users. This feature uses an offline detect timer to set the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.

Restrictions and guidelines

The 802.1X offline detection feature takes effect only on a port that performs MAC-based access control. If you change the port access mode to port-based, the 802.1X offline detection feature cannot take effect.

For this feature to operate as expected, do not set the offline detect timer to the same value as either of the following timers:

- Handshake timer (set by using the **dot1x timer handshake-period** command).
- Periodic reauthentication timer (set by using the **dot1x timer reauth-period** command).

Procedure

1. Enter system view.
   system-view
2. Set the 802.1X offline detect timer.
   dot1x timer offline-detect *offline-detect-value*
   By default, the 802.1X offline detect timer is 300 seconds.
3. Enter interface view.
   interface *interface-type interface-number*
4. Enable 802.1X offline detection.
   dot1x offline-detect enable
   By default, 802.1X offline detection is disabled.

Command reference

dot1x offline-detect enable

Use **dot1x offline-detect enable** to enable 802.1X offline detection on a port.

Use **undo dot1x offline-detect enable** to disable 802.1X offline detection.

Syntax

dot1x offline-detect enable

undo dot1x offline-detect enable

Default

802.1X offline detection is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The 802.1X offline detection feature monitors the online status of 802.1X users. This feature uses an offline detect timer to set the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user.

To have 802.1X offline detection take effect, you must configure the port to perform MAC-based access control. If you change the port access mode to port-based, the 802.1X offline detection feature cannot take effect.

To set the offline detect timer, use the **dot1x timer** command.

Examples

Disable 802.1X offline detection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x offline-detect enable
```

Related commands

display dot1x

dot1x port-method

dot1x timer

dot1x timer offline-detect

Use **dot1x timer offline-detect** to set the 802.1X offline detect timer.

Use **undo dot1x timer offline-detect** to restore the default.

Syntax

dot1x timer offline-detect *offline-detect-value*

undo dot1x timer offline-detect

Default

The 802.1X offline detect timer is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

offline-detect *offline-detect-value*: Sets the offline detect timer in seconds. The value range for the *offline-detect-value* argument is 60 to 2147483647.

Usage guidelines

The offline detect timer sets the interval that the device waits for traffic from a user before the device determines that the user is idle. If the device has not received traffic from a user before the timer expires, the device logs off that user and requests the accounting server to stop accounting for the user. This timer takes effect only when the 802.1X offline detection feature is enabled.

Examples

Set the 802.1X offline detect timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer offline-detect 150
```

Related commands

display dot1x

New feature: Enabling SAVI and setting the entry deletion delay by using commands

The ipv6 savi strict and ipv6 savi down-delay commands were added. You can use these commands to enable SAVI and set the entry deletion delay.

About SAVI

Source Address Validation Improvement (SAVI) checks the validity of the source addresses of global unicast IPv6 packets. It implements the validity check by using the ND snooping, DHCPv6 snooping, ND attack detection, and IP source guard features. SAVI checks only global unicast addresses and forwards the packets that pass the validity check. Packets sourced from an invalid address are dropped.

SAVI application scenarios

DHCPv6-only

The hosts connected to the SAVI-enabled device obtain addresses only through DHCPv6. In this scenario, SAVI drops all RA and RR messages. DHCPv6 messages, ND messages (RA and RR messages excluded), and IPv6 data packets are checked based on DHCPv6 snooping entries and static IPv6 source guard binding entries.

SLAAC-only

The hosts connected to the SAVI-enabled device obtain addresses only through Stateless Address Autoconfiguration (SLAAC). In this scenario, SAVI drops all DHCPv6 messages. Only ND messages and IPv6 data packets are checked based on DHCPv6 snooping entries and static IPv6 source guard binding entries.

DHCPv6+SLAAC

The hosts connected to the SAVI-enabled device obtain addresses through DHCPv6 and SLAAC. In this scenario, SAVI checks all DHCPv6 messages, ND messages, and IPv6 data packets based on DHCPv6 snooping entries, ND snooping entries, and static IPv6 source guard binding entries.

SAVI tasks at a glance

To configure SAVI, perform the following tasks:

1. Enabling SAVI
2. Configuring IPv6 source guard
3. Configuring DHCPv6 snooping
4. Configuring ND snooping and ND attack detection
5. (Optional.) Setting the entry deletion delay

Enabling SAVI

1. Enter system view.

   system-view
2. Enable SAVI.

   ipv6 savi strict

   By default, SAVI is disabled.

Configuring IPv6 source guard

1. Enable IPv6 source guard on an interface.
2. (Optional.) Configure static IPv6SG bindings.

For more information about IPv6 source guard configuration, see "Configuring IP source guard."

Configuring DHCPv6 snooping

Restrictions and guidelines

Enable only DHCPv6 snooping for the SLAAC-only scenario.

Procedure

1. Enable DHCPv6 snooping.
2. Specify DHCPv6 snooping trusted ports.
3. Enable recording client information in DHCPv6 snooping entries.

For more information about DHCPv6 snooping configuration, see *Layer 3—IP Services Configuration Guide*.

Configuring ND snooping and ND attack detection

Restrictions and guidelines

Enable only ND attack detection for the DHCPv6-only scenario.

Procedure

1. Enable ND snooping for global unicast addresses.

   For more information about ND snooping, see IPv6 basics in *Layer 3—IP Services Configuration Guide*.
2. Enable ND attack detection.

   For more information about ND attack detection, see "Configuring ND attack defense."
3. Specify ND trusted ports.

   For more information about ND trusted ports, see "Configuring ND attack defense."

Setting the entry deletion delay

About the entry deletion delay

The entry deletion delay is the period of time that the device waits before deleting the DHCPv6 snooping entries and ND snooping entries for a down port.

Procedure

1. Enter system view.

   system-view
2. Set the entry deletion delay.

   ipv6 savi down-delay *delay-time*

   By default, the entry deletion delay is 30 seconds.

SAVI configuration examples

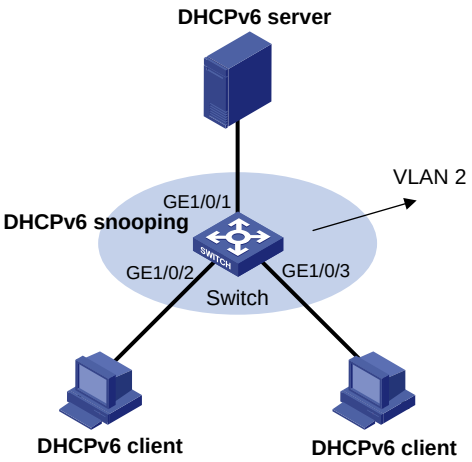
Example: Configuring DHCPv6-only SAVI

Network configuration

As shown in Figure 1, configure SAVI on the switch to meet the following requirements:

- Clients obtain IPv6 addresses only through DHCPv6.
- RA and RR messages are dropped on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 in VLAN 2.
- SAVI checks the source addresses of DHCPv6 messages, ND messages (RA and RR messages excluded), and IPv6 data packets on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

Figure 1 Network diagram



Procedure

Enable SAVI.

```
<Switch> system-view
[Switch] ipv6 savi strict
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
[Switch-vlan2] quit
```

Enable DHCPv6 snooping.

```
[Switch] ipv6 dhcp snooping enable
```

Configure GigabitEthernet 1/0/1 as a DHCPv6 snooping trusted port.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
[Switch-GigabitEthernet1/0/1] quit
```

Enable recording DHCPv6 snooping entries on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ipv6 dhcp snooping binding record
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] ipv6 dhcp snooping binding record
[Switch-GigabitEthernet1/0/3] quit
```

Enable ND attack detection.

```
[Switch] vlan 2
[Switch-vlan2] ipv6 nd detection enable
[Switch-vlan2] quit
```

Enable IPv6 source guard on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ipv6 verify source ip-address mac-address
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] ipv6 verify source ip-address mac-address
[Switch-GigabitEthernet1/0/3] quit
```

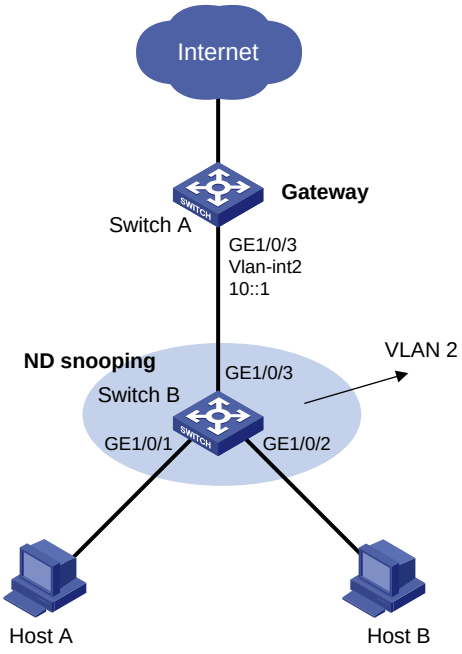
Example: Configuring SLAAC-only SAVI

Network configuration

As shown in Figure 2, configure SAVI on Switch B to meet the following requirements:

- Hosts obtain IPv6 addresses only through SLAAC.
- DHCPv6 messages are dropped on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 in VLAN 2.
- SAVI checks the source addresses of ND messages and IPv6 data packets on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

Figure 2 Network diagram



Procedure

Enable SAVI.

```
<SwitchB> system-view
[SwitchB] ipv6 savi strict
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
[SwitchB-vlan2] quit
```

Enable ND snooping for global unicast addresses in VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] ipv6 nd snooping enable global
```

Enable ND attack detection for VLAN 2.

```
[SwitchB-vlan2] ipv6 nd detection enable
[SwitchB-vlan2] quit
```

Enable DHCPv6 snooping.

```
[SwitchB] ipv6 dhcp snooping enable
```

Configure GigabitEthernet 1/0/3 as an ND trusted port.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 nd detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

Enable IPv6 source guard on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchB-GigabitEthernet1/0/2] quit
```

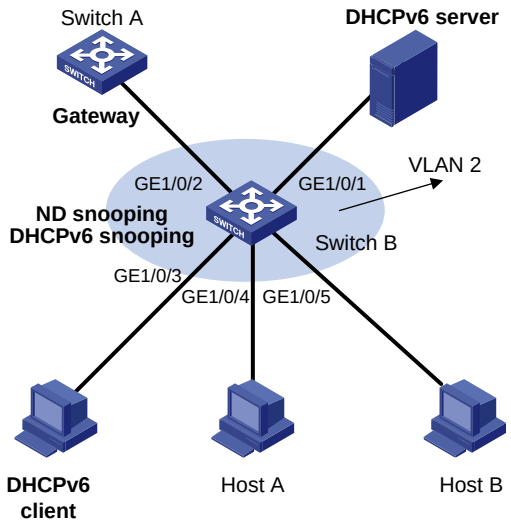
Example: Configuring DHCPv6+SLAAC SAVI

Network configuration

As shown in Figure 3, configure SAVI on Switch B to meet the following requirements:

- Hosts obtain IP addresses through DHCPv6 or SLAAC.
- SAVI checks the source addresses of DHCPv6 messages, ND messages, and IPv6 data packets on GigabitEthernet 1/0/3 through GigabitEthernet 1/0/5.

Figure 3 Network diagram



Procedure

Enable SAVI.

```
<SwitchB> system-view
[SwitchB] ipv6 savi strict
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
gigabitethernet 1/0/4 gigabitethernet 1/0/5
```

Enable DHCPv6 snooping.

```
[SwitchB] ipv6 dhcp snooping enable
```

Enable recording DHCPv6 snooping entries on GigabitEthernet 1/0/3 through GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 dhcp snooping binding record
[SwitchB-GigabitEthernet1/0/3] quit
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ipv6 dhcp snooping binding record
[SwitchB-GigabitEthernet1/0/4] quit
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] ipv6 dhcp snooping binding record
[SwitchB-GigabitEthernet1/0/5] quit
```

Configure GigabitEthernet 1/0/1 as a DHCPv6 snooping trusted port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Enable ND snooping for global unicast addresses in VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] ipv6 nd snooping enable global
```

Enable ND attack detection for VLAN 2.

```
[SwitchB-vlan2] ipv6 nd detection enable
[SwitchB-vlan2] quit
```

Configure GigabitEthernet 1/0/2 as an ND trusted port.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ipv6 nd detection trust
[SwitchB-GigabitEthernet1/0/2] quit
```

Enable IPv6 source guard on GigabitEthernet 1/0/3 through GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ip verify source ipv6 ip-address mac-address
[SwitchB-GigabitEthernet1/0/3] quit
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ip verify source ipv6 ip-address mac-address
[SwitchB-GigabitEthernet1/0/4] quit
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] ip verify source ipv6 ip-address mac-address
```

SAVI commands

ipv6 savi down-delay

Use **ipv6 savi down-delay** to set the entry deletion delay.

Use **undo ipv6 savi down-delay** to restore the default.

Syntax

ipv6 savi down-delay *delay-time*

undo ipv6 savi down-delay

Default

The entry deletion delay is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the entry deletion delay in the range of 0 to 21474836 seconds.

Usage guidelines

The entry deletion delay is the period of time that the device waits before deleting the DHCPv6 snooping entries and ND snooping entries for a down port.

Examples

Set the entry deletion delay to 100 seconds.

```
<Sysname> system-view
[Sysname] ipv6 savi down-delay 100
```

ipv6 savi strict

Use **ipv6 savi strict** to enable Source Address Validation Improvement (SAVI).

Use **undo ipv6 savi strict** to disable SAVI.

Syntax

ipv6 savi strict

undo ipv6 savi strict

Default

SAVI is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable SAVI.

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi strict
```

Related commands

ipv6 verify source

Modified feature: Configuring MAC-based MAC authentication user accounts

Feature change description

Support for password configuration was added to MAC-based MAC authentication user accounts.

Command changes

Modified command: mac-authentication user-name-format

Old syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }

New syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] [**password** { **cipher** | **simple** } *string*] }

Views

System view

Change description

Before modification: You cannot specify a password for MAC-based MAC authentication user accounts. The MAC address of each user is used as the password.

After modification: You can specify a password for all MAC-based MAC authentication user accounts by using the **password** { **cipher** | **simple** } *string* option. If you do not specify a password, each user uses its own MAC address as the password.

- **password**: Specifies the password for MAC-based MAC authentication user accounts.
- **cipher**: Specifies a password in encrypted form.
- **simple**: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.
- *string*: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Modified feature: Port security NTK feature

Feature change description

In this release, the ntkauto mode was added to the need to known (NTK) feature of port security.

Command changes

Modified command: port-security ntk-mode

Old syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

New syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkauto** | **ntkonly** }

Views

Layer 2 Ethernet interface view

Change description

Before modification: The **ntkauto** keyword was not added to this command.

After modification: The **ntkauto** keyword was not added to this command. This keyword specifies the ntkauto mode. A port in ntkauto mode forwards broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses only when the port has online users.

Release 3208P08

This release has the following changes:

New feature: Shutting down an interface by OpenFlow

New feature: Shutting down an interface by OpenFlow

Shut down an interface by OpenFlow.

About interface shutdown

After an interface is shut down by OpenFlow, the **Current state** field displays **OFP DOWN** in the **display interface** command output.

You can use the **undo openflow shutdown** command to bring up an interface shut down by OpenFlow. The interface can also be brought up by port modification messages from controllers.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Shut down an interface by OpenFlow.
   openflow shutdown
   By default, an interface is not shut down by OpenFlow.

Command reference

openflow shutdown

Use **openflow shutdown** to shut down an interface by OpenFlow.

Use **undo openflow shutdown** to restore the default.

Syntax

openflow shutdown

undo openflow shutdown

Default

An interface is not shut down by OpenFlow.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After an interface is shut down by OpenFlow, the **Current state** field displays **OFP DOWN** in the **display interface** command output.

To bring up an interface shut down by OpenFlow, use either of the following methods:

- Use the **undo openflow shutdown** command on the interface.
- Use the controller to send port modification messages to the interface.

Examples

Shut down GigabitEthernet 1/0/1 by OpenFlow.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] openflow shutdown
```

Release 3208P03

This release has the following changes:

New feature: VRRP

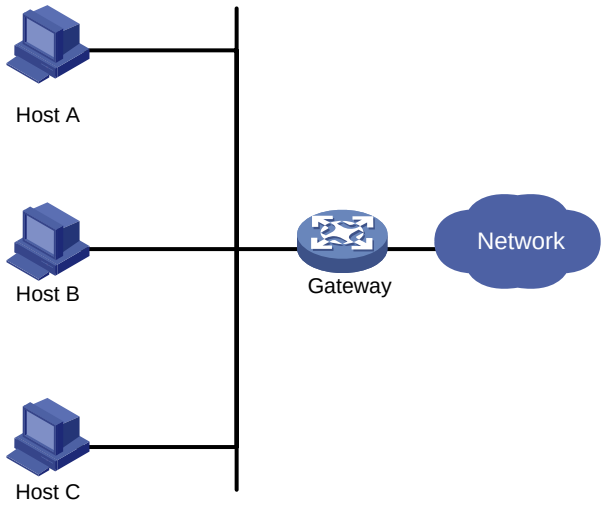
New feature: VRRP

VRRP does not take effect on member ports of aggregation groups.

About VRRP

Typically, you can configure a default gateway for every host on a LAN. All packets destined for other networks are sent through the default gateway. As shown in Figure 1, when the default gateway fails, no hosts can communicate with external networks.

Figure 1 LAN networking



Using a default gateway facilitates your configuration but requires high availability. Using more egress gateways improves link availability but introduces the problem of routing among the egresses.

Virtual Router Redundancy Protocol (VRRP) is designed to address this issue. VRRP adds a group of network gateways to a VRRP group called a virtual router. The VRRP group has one master and multiple backups, and provides a virtual IP address. The hosts on the subnet use the virtual IP address as their default network gateway to communicate with external networks.

VRRP avoids single points of failure and simplifies the configuration on hosts. When the master in the VRRP group on a multicast or broadcast LAN (for example, an Ethernet network) fails, another router in the VRRP group takes over. The switchover is complete without causing dynamic route recalculation, route re-discovery, gateway reconfiguration on the hosts, or traffic interruption.

VRRP operates in either of the following modes:

- **Standard mode**—Implemented based on RFCs. For more information, see "VRRP standard mode."
- **Load balancing mode**—Extends the VRRP standard mode to distribute load across VRRP group members. For more information, see "VRRP load balancing mode."

VRRP has two versions: VRRPv2 and VRRPv3. VRRPv2 supports IPv4 VRRP. VRRPv3 supports IPv4 VRRP and IPv6 VRRP.

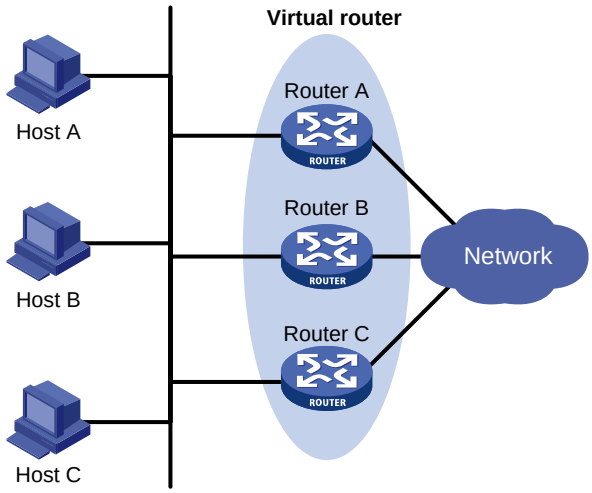
VRRP standard mode

VRRP networking

As shown in Figure 2, Router A, Router B, and Router C form a virtual router, which has its own IP address. Hosts on the subnet use the virtual router as the default gateway.

The router with the highest priority among the three routers is elected as the master, and the other two are backups. Only the master in the VRRP group can provide gateway service. When the master fails, the backup routers elect a new master to take over for nonstop gateway service.

Figure 2 VRRP networking



Virtual IP address and IP address owner

The virtual IP address of the virtual router can be either of the following IP addresses:

- Unused IP address on the subnet where the VRRP group resides.
- IP address of an interface on a router in the VRRP group.

In the latter case, the router is called the IP address owner. A VRRP group can have only one IP address owner.

Router priority in a VRRP group

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with higher priority is more likely to become the master.

A VRRP priority can be in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Preemption

A router in a VRRP group operates in either non-preemptive mode or preemptive mode.

- **Non-preemptive mode**—The master router acts as the master as long as it operates correctly, even if a backup router is later assigned a higher priority. Non-preemptive mode helps avoid frequent switchover between the master and backup routers.
- **Preemptive mode**—A backup starts a new master election and takes over as master when it detects that it has a higher priority than the current master. Preemptive mode ensures that the router with the highest priority in a VRRP group always acts as the master.

Authentication method

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication methods:

- Simple authentication

  The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

- MD5 authentication

  The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the packet. The receiver performs the same operation with the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and gets discarded.

On a secure network, you can choose to not authenticate VRRP packets.

NOTE:

IPv4 VRRPv3 and IPv6 VRRPv3 do not support VRRP packet authentication.

VRRP timers

Skew_Time

Skew_Time helps avoid the situation that multiple backups in a VRRP group become the master when the master in the VRRP group fails.

Skew_Time is not configurable; its value depends on the VRRP version.

- In VRRPv2 (described in RFC 3768), Skew_Time is (256 – Router priority)/256.
- In VRRPv3 (described in RFC 5798), Skew_Time is ((256 – Router priority) × VRRP advertisement interval)/256.

VRRP advertisement interval

The master in a VRRP group periodically sends VRRP advertisements to declare its presence.

You can configure the interval at which the master sends VRRP advertisements. If a backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement interval + Skew_Time) expires, it takes over as the master.

VRRP preemption delay timer

You can configure the VRRP preemption delay timer for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

In preempt mode, a backup does not immediately become the master after it receives an advertisement with lower priority than the local priority. Instead, it waits for a period of time (preemption delay time + Skew_Time) before taking over as the master.

Master election

Routers in a VRRP group determine their roles by priority. When a router joins a VRRP group, it has a backup role. The router role changes according to the following situations:

- If the backup does not receive any VRRP advertisement when the timer (3 × advertisement interval + Skew_Time) expires, it becomes the master.
- If the backup receives a VRRP advertisement with the same or greater priority within the timer (3 × advertisement interval + Skew_Time), it remains a backup.
- If the backup receives a VRRP advertisement with a smaller priority within the timer (3 × advertisement interval + Skew_Time), the following results apply:
  - It remains a backup when operating in non-preemptive mode.
  - It becomes the master when operating in preemptive mode.

The elected master starts a VRRP advertisement interval to periodically send VRRP advertisements to notify the backups that it is operating correctly. Each of the backups starts a timer to wait for advertisements from the master.

When multiple routers in a VRRP group declare that they are the master because of network problems, the one with the highest priority becomes the master. If two routers have the same priority, the one with the highest IP address becomes the master.

VRRP tracking

The VRRP tracking function uses network quality analyzer (NQA) or bidirectional forwarding detection (BFD) to monitor the state of the master or the upstream link. The collaboration between VRRP and NQA or BFD through a track entry implements the following functions:

- Monitors the upstream link and changes the priority of the router according to the state of the link. If the upstream link fails, the hosts on the subnet cannot access external networks through the router and the state of the track entry becomes Negative. The priority of the master decreases by a specified value, and a router with a higher priority in the VRRP group becomes the master. The switchover ensures uninterrupted communication between the hosts on the subnet and external networks.
- Monitors the state of the master on the backups. When the master fails, a backup immediately takes over to ensure uninterrupted communication.

When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority. For more information about track entries, see "Configuring Track."

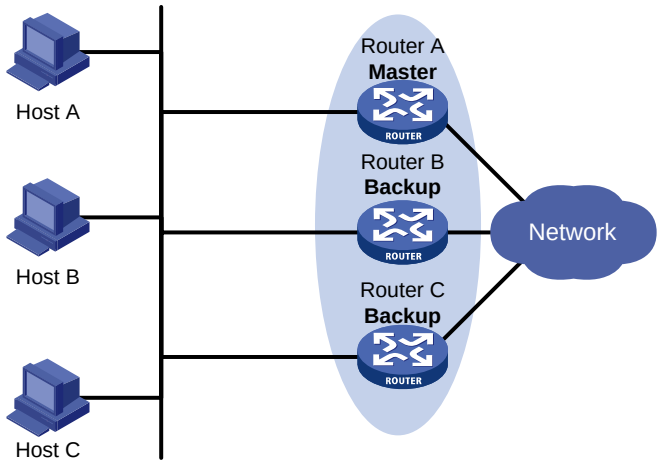
To enable VRRP tracking, configure the routers in the VRRP group to operate in preemptive mode first. This configuration ensures that only the router with the highest priority operates as the master.

VRRP application

Master/backup

In master/backup mode, only the master forwards packets, as shown in Figure 3. When the master fails, a new master is elected from among the backups. This mode requires only one VRRP group, and each router in the group has a different priority. The one with the highest priority becomes the master.

Figure 3 VRRP in master/backup mode



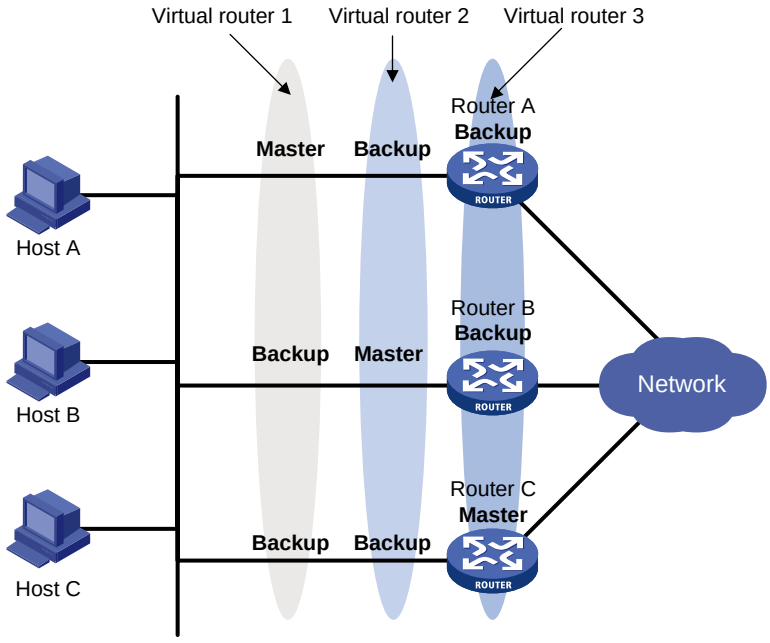
Assume that Router A is acting as the master to forward packets to external networks, and Router B and Router C are backups in listening state. When Router A fails, Router B and Router C elect a new master to forward packets for hosts on the subnet.

Load sharing

A router can join multiple VRRP groups. With different priorities in different VRRP groups, the router can act as the master in one VRRP group and a backup in another.

In load sharing mode, multiple VRRP groups provide gateway services. This mode requires a minimum of two VRRP groups, and each group has one master and multiple backups. The master roles in the VRRP groups are assumed by different routers, as shown in Figure 4.

Figure 4 Load sharing of VRRP



A router can be in multiple VRRP groups and have a different priority in each group.

As shown in Figure 4, the following VRRP groups exist:

- **VRRP group 1**—Router A is the master. Router B and Router C are the backups.
- **VRRP group 2**—Router B is the master. Router A and Router C are the backups.

- **VRRP group 3**—Router C is the master. Router A and Router B are the backups.

To implement load sharing among Router A, Router B, and Router C, perform the following tasks:

- Configure the virtual IP addresses of VRRP group 1, 2, and 3 as default gateway IP addresses for hosts on the subnet.
- Assign the highest priority to Router A, B, and C in VRRP group 1, 2, and 3, respectively.

VRRP load balancing mode

In a standard-mode VRRP group, only the master can forward packets and backups are in listening state. You can create multiple VRRP groups to share traffic, but you must configure different gateways for hosts on the subnet.

In load balancing mode, a VRRP group maps its virtual IP address to multiple virtual MAC addresses, assigning one virtual MAC address to each member router. Every router in this VRRP group can forward traffic and respond to IPv4 ARP requests or IPv6 ND requests from hosts. Because their virtual MAC addresses are different, traffic from hosts is distributed across the VRRP group members. Load balancing mode simplifies configuration and improves forwarding efficiency.

VRRP load balancing mode uses the same master election, preemption, and tracking mechanisms as the standard mode. New mechanisms have been introduced to VRRP load balancing mode, as described in the following sections.

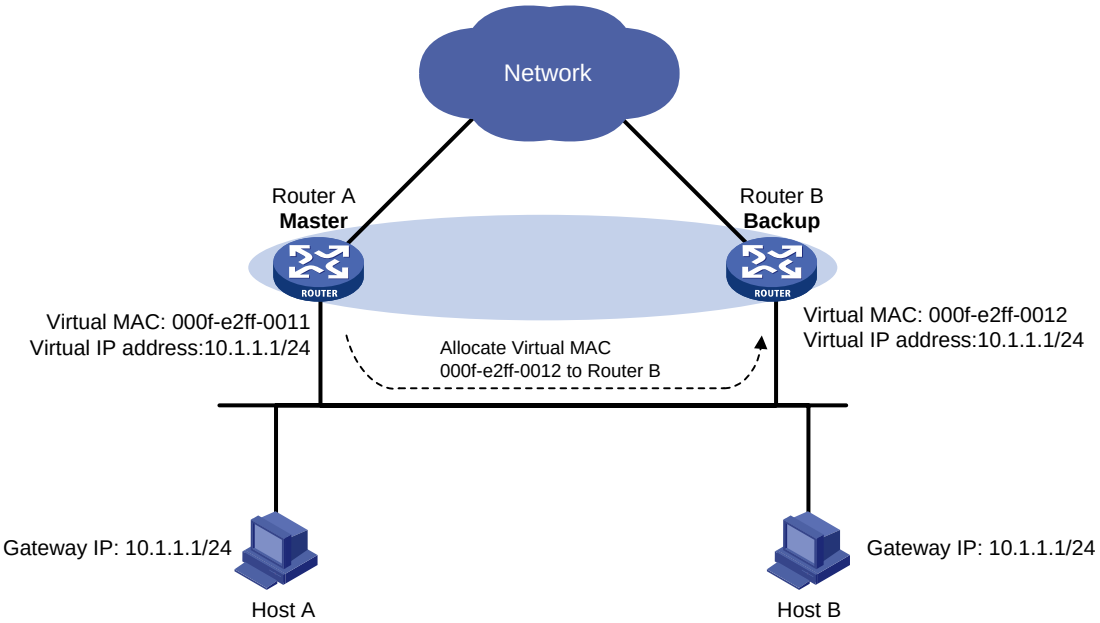
Virtual MAC address assignment

In load balancing mode, the master assigns virtual MAC addresses to routers in the VRRP group. The master uses different MAC addresses to respond to ARP requests or ND requests from different hosts. The backup routers, however, do not answer ARP requests or ND requests from hosts.

In an IPv4 network, a load balanced VRRP group works as follows:

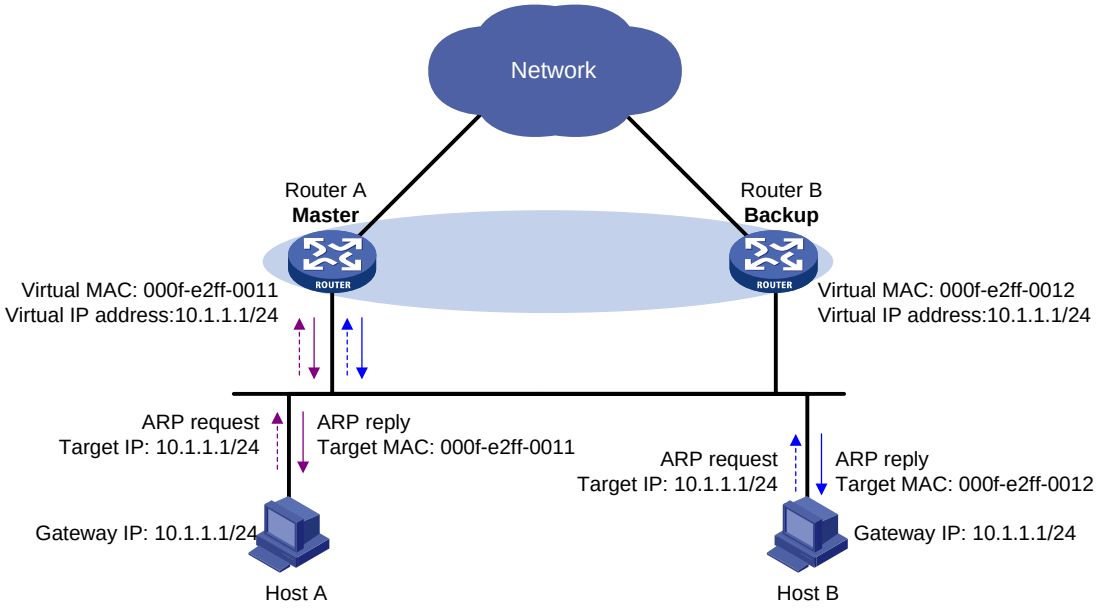
1. The master assigns virtual MAC addresses to all member routers, including itself. This example assumes that the virtual IP address of the VRRP group is 10.1.1.1/24, Router A is the master, and Router B is the backup. Router A assigns 000f-e2ff-0011 for itself and 000f-e2ff-0012 for Router B. See Figure 5.

Figure 5 Virtual MAC address assignment



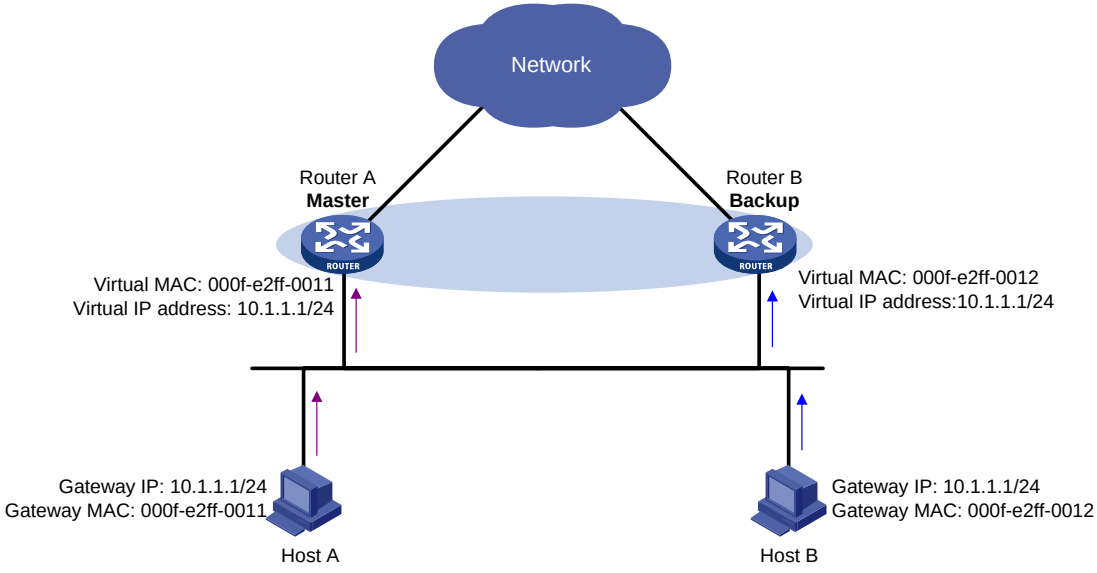
2. When an ARP request arrives, the master (Router A) selects a virtual MAC address based on the load balancing algorithm to answer the ARP request. In this example, Router A returns the virtual MAC address of itself in response to the ARP request from Host A. Router A returns the virtual MAC address of Router B in response to the ARP request from Host B. See Figure 6.

Figure 6 Answering ARP requests



3. Each host sends packets to the returned MAC address. As shown in Figure 7, Host A sends packets to Router A and Host B sends packets to Router B.

Figure 7 Sending packets to different routers for forwarding



In the ARP reply sent by the master, the source MAC address in the Ethernet header is different from the sender MAC address in the message body. For the Layer 2 device to forward the ARP packet, follow these configuration guidelines on the Layer 2 device:

- Do not enable ARP packet source MAC address consistency check.
- Do not specify the **src-mac** keyword when you enable ARP packet validity check for ARP detection.

For more information about ARP packet source MAC address consistency check and ARP detection, see *Security Configuration Guide*.

Virtual forwarder

Virtual forwarder creation

Virtual MAC addresses enable traffic distribution across routers in a VRRP group. To enable routers in the VRRP group to forward packets, VFs must be created on them. Each VF is associated with a virtual MAC address in the VRRP group and forwards packets that are sent to this virtual MAC address.

VFs are created on routers in a VRRP group, as follows:

1. The master assigns virtual MAC addresses to all routers in the VRRP group. Each member router creates a VF for this MAC address and becomes the owner of this VF.
2. Each VF owner advertises its VF information to the other member routers.
3. After receiving the VF advertisement, each of the other routers creates the advertised VF.

Eventually, every member router maintains one VF for each virtual MAC address in the VRRP group.

VF weight and priority

The weight of a VF indicates the forwarding capability of a VF. A higher weight means higher forwarding capability. When the weight is lower than the lower limit of failure, the VF cannot forward packets.

The priority of a VF determines the VF state. Among the VFs created on different member routers for the same virtual MAC address, the VF with the highest priority is in active state. This VF, known as the active virtual forwarder (AVF), forwards packets. All other VFs listen to the state of the AVF and are known as the listening virtual forwarders (LVFs). VF priority is in the range of 0 to 255, where 255 is reserved for the VF owner. When the weight of a VF owner is higher than or equal to the lower limit of failure, the priority of the VF owner is 255.

The priority of a VF is calculated based on its weight.

- If the VF weight is higher than or equal to the lower limit of failure, the following VF priorities apply:
  - On a VF owner, the VF priority is 255.
  - On a non-VF owner, the VF priority is calculated as weight/(number of local AVFs + 1).
- If the VF weight is lower than the lower limit of failure, the VF priority is 0.

VF backup

The VFs corresponding to a virtual MAC address on different routers in the VRRP group back up one another.

Figure 8 VF information

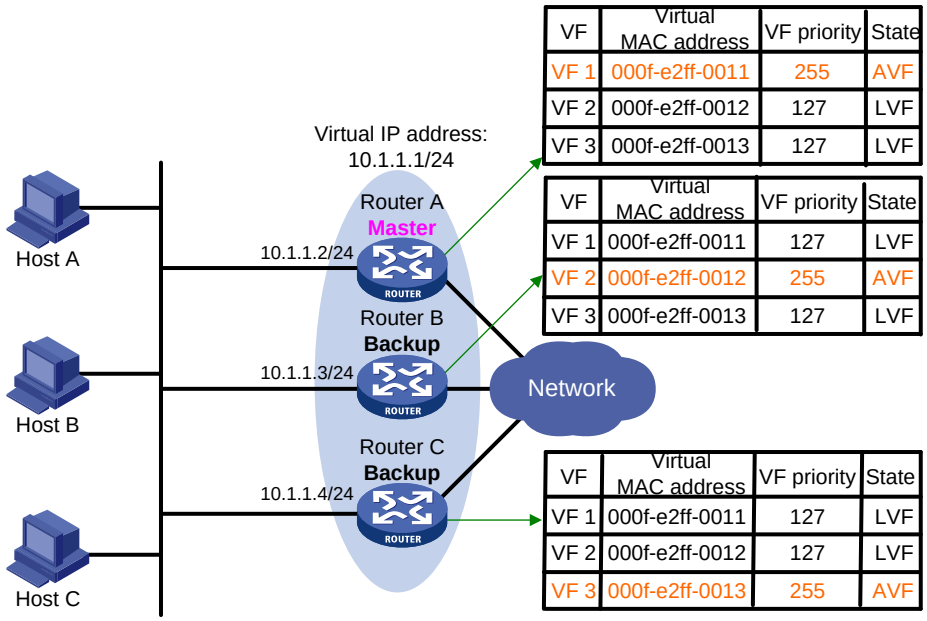


Figure 8 shows the VF table on each router in the VRRP group and how the VFs back up one another. The master, Router A, assigns virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013 to itself, Router B, and Router C, respectively. Each router creates VF 1, VF 2, and VF 3 for virtual MAC addresses 000f-e2ff-0011, 000f-e2ff-0012, and 000f-e2ff-0013, respectively. The VFs for the same virtual MAC address on different routers back up one another. For example, the VF 1 instances on Router A, Router B, and Router C back up one another.

- The VF 1 instance on Router A (the VF 1 owner) has priority 255. It acts as the AVF to forward packets sent to virtual MAC address 000f-e2ff-0011.
- The VF 1 instances on Router B and Router C have a priority of 255/(1 + 1), or 127. Because their priorities are lower than the priority of the VF 1 instance on Router A, they act as LVFs. These LVFs listen to the state of the VF 1 instance on Router A.
- When the VF 1 instance on Router A fails, the VF 1 instances on Router B and Router C elect the one with higher priority as the new AVF. This AVF forwards packets destined for virtual MAC address 000f-e2ff-0011. If the two LVFs' priorities are the same, the LVF with a greater device MAC address becomes the new AVF.

A VF always operates in preemptive mode. When an LVF finds its priority value higher than the one advertised by the AVF, the LVF declares itself as the AVF.

VF timers

When the AVF on a router fails, the new AVF on another router creates the following timers for the failed AVF:

- **Redirect timer**—Before this timer expires, the master still uses the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts. The VF owner can share traffic load if the VF owner resumes normal operation within this time. When this timer expires, the master stops using the virtual MAC address corresponding to the failed AVF to respond to ARP/ND requests from hosts.
- **Timeout timer**—The duration after which the new AVF takes over responsibilities of the failed VF owner. Before this timer expires, all routers in the VRRP group keep the VFs that correspond to the failed AVF. The new AVF forwards packets destined for the virtual MAC address of the failed AVF. When this timer expires, all routers in the VRRP group remove the VFs that correspond to the failed AVF, including the new AVF. Packets destined for the virtual MAC address of the failed AVF are not forwarded any longer.

VF tracking

An AVF forwards packets destined for the MAC address of the AVF. If the AVF's upstream link fails but no LVF takes over, the hosts that use the AVF's MAC address as their gateway MAC address cannot access the external network.

The VF tracking function can solve this problem. You can use NQA or BFD to monitor the upstream link state of the VF owner, and associate the VFs with NQA or BFD through the tracking function. This enables the collaboration between VRRP and NQA or BFD through the Track module. When the upstream link fails, the state of the track entry changes to Negative. The weights of the VFs (including the AVF) on the router decrease by a specific value. The corresponding LVF with a higher priority on another router becomes the AVF and forwards packets.

Protocols and standards

- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*

Configuring IPv4 VRRP

Restrictions and guidelines: IPv4 VRRP configuration

- IPv4 VRRP does not take effect on member ports of aggregation groups.
- Configuration on the routers in an IPv4 VRRP group must be consistent.

IPv4 VRRP tasks at a glance

To configure IPv4 VRRP, perform the following tasks:

1. Specifying an IPv4 VRRP operating mode
2. (Optional.) Specifying the IPv4 VRRP version
3. Configuring an IPv4 VRRP group
4. (Optional.) Configuring IPv4 VRRP packet attributes
5. (Optional.) Configuring VF tracking
6. This configuration takes effect only in VRRP load balancing mode.
7. (Optional.) Setting the packet sending mode for IPv4 VRRPv3
8. (Optional.) Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP
9. (Optional.) Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group
10. (Optional.) Enabling SNMP notifications for VRRP

Specifying an IPv4 VRRP operating mode

Restrictions and guidelines

After an IPv4 VRRP operating mode is configured on a router, all IPv4 VRRP groups on the router operate in the specified operating mode.

Procedure

1. Enter system view.

   system-view
2. Specify an IPv4 VRRP operating mode.
   - Specify the standard mode.

- **undo vrrp mode**
- Specify the load balancing mode.
- **vrrp mode load-balance** [**version-8**]

By default, VRRP operates in standard mode.

Specifying the IPv4 VRRP version

About IPv4 VRRP versions

IPv4 VRRP can use VRRPv2 and VRRPv3.

Restrictions and guidelines

For an IPv4 VRRP group to operate correctly, make sure the same VRRP version is used on all routers in the IPv4 VRRP group.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Specify the version of VRRP.
   vrrp version *version-number*
   By default, VRRPv3 is used.

Configuring an IPv4 VRRP group

About IPv4 VRRP group

A VRRP group can operate correctly after you create it and assign a minimum of one virtual IP address to it. You can configure multiple virtual IP addresses for the VRRP group on an interface that connects to multiple subnets for router backup on different subnets.

If you disable an IPv4 VRRP group, the VRRP group enters initialized state, and the existing configuration on the VRRP group remains unchanged. You can modify the configuration of the VRRP group. The modification takes effect when you enable the VRRP group again.

Restrictions and guidelines

Item	Remarks
VLAN interface	Do not create a VRRP group on the VLAN interface of a super VLAN because network performance might be adversely affected. For information about the super VLAN feature, see *Layer 2—LAN Switching Configuration Guide*.
Maximum number of VRRP groups and virtual IP addresses	In VRRP load balancing mode, the device supports a maximum of *MaxVRNum/N* VRRP groups. *MaxVRNum* refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. *N* refers to the number of devices in the VRRP group.
Virtual IP address	When VRRP is operating in standard mode, the virtual IP address of a VRRP group can be either of the following addresses: • Unused IP address on the subnet where the VRRP group resides. • IP address of an interface on a router in the VRRP group. In load balancing mode, the virtual IP address of a VRRP group can be any unassigned IP address of the subnet where the VRRP group resides. It cannot be the IP address of any interfaces in the VRRP

Item	Remarks
	group. No IP address owner can exist in a VRRP group. An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function. For hosts in the subnet to access external networks, as a best practice, configure the following addresses in the same subnet: • Virtual IP address of an IPv4 VRRP group. • Downlink interface IP addresses of the VRRP group members.
IP address owner	On an IP address owner, as a best practice, do not use the **network** command to enable OSPF on the interface owning the virtual IP address of the VRRP group. For more information about the **network** command, see *Layer 3—IP Routing Command Reference*. Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface. The running priority of an IP address owner is always 255, and you do not need to configure it. An IP address owner always operates in preemptive mode. If you configure the **vrrp vrid track priority reduced** or **vrrp vrid track switchover** command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner.
VRRP association with a track entry	When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority or the failed master router becomes the master again.

Creating a VRRP group and assigning a virtual IP address

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Create a VRRP group and assign a virtual IP address.
   vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

Configuring an IPv4 VRRP group

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Set the priority of the router in the VRRP group.
   vrrp vrid *virtual-router-id* **priority** *priority-value*
   The default setting is 100.
4. Enable the preemptive mode for the router in a VRRP group and set the preemption delay time.
   vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]
   By default, the router in a VRRP group operates in preemptive mode and the preemption delay time is 0 centiseconds, which means an immediate preemption.

5. Associate a VRRP group with a track entry.

   vrrp vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

   By default, a VRRP group is not associated with any track entries.

Disabling an IPv4 VRRP group

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Disable a VRRP group.

   vrrp vrid *virtual-router-id* **shutdown**

Configuring IPv4 VRRP packet attributes

Restrictions and guidelines

- You can configure different authentication modes and authentication keys for VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
- In VRRPv2, all routers in a VRRP group must have the same VRRP advertisement interval.
- In VRRPv3, authentication mode and authentication key settings do not take effect.
- In VRRPv3, routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at specified intervals, and carries the interval in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Configure the authentication mode and authentication key for an IPv4 VRRP group to send and receive VRRP packets.

   vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *string*

   By default, authentication is disabled.

4. Set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

   vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

   The default setting is 100 centiseconds.

   As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

5. Specify the source interface for receiving and sending VRRP packets.

   vrrp vrid *virtual-router-id* **source-interface** *interface-type interface-number*

   By default, the source interface for receiving and sending VRRP packets is not specified. The interface where the VRRP group resides sends and receives VRRP packets.

6. Enable TTL check for IPv4 VRRP packets.

   vrrp check-ttl enable

   By default, TTL check for IPv4 VRRP packets is enabled.

7. Return to system view.

   quit

8. Set a DSCP value for VRRP packets.

   vrrp dscp *dscp-value*

   By default, the DSCP value for VRRP packets is 48.

   The DSCP value identifies the packet priority during transmission.

Configuring VF tracking

About VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can establish the collaboration between the VFs and NQA or BFD through the tracking function. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weight values of the VFs restore.

Restrictions and guidelines

- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Configure the VFs in a VRRP group to monitor a track entry.

   vrrp vrid *virtual-router-id* **track** *track-entry-number*
   { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

   By default, no track entry is specified.

Setting the packet sending mode for IPv4 VRRPv3

About the packet sending mode for IPv4 VRRPv3

A router configured with VRRPv3 can process incoming VRRPv2 packets, but a router configured with VRRPv2 cannot process incoming VRRPv3 packets. When the VRRP version of the routers in a VRRP group is changed from VRRPv2 to VRRPv3, multiple masters might be elected in the VRRP group. To resolve the problem, you can set the packet sending mode for IPv4 VRRPv3. This task enables a router configured with VRRPv3 to send VRRPv2 packets and communicate with routers configured with VRRPv2.

Restrictions and guidelines

- The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.
- If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.
- The VRRP advertisement interval is set in centiseconds by using the **vrrp vrid timer advertise** command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the **vrrp vrid timer advertise** command in *High Availability Command Reference*.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Set the packet sending mode for IPv4 VRRPv3.

   vrrp vrid *virtual-router-id* **vrrpv3-send-packet** { **v2-only** | **v2v3-both** }

   By default, a router configured with VRRPv3 sends only VRRPv3 packets.

Enabling periodic sending of gratuitous ARP packets for IPv4 VRRP

About periodic sending of gratuitous ARP packets for IPv4 VRRP

This feature enables the master router in a VRRP group to periodically send gratuitous ARP packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the VRRP group in a timely manner.

Restrictions and guidelines

- This feature takes effect only in VRRP standard mode.
- If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.
- The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the **vrrp send-gratuitous-arp** command. This prevents too many gratuitous ARP packets from being sent at the same time.
- The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:
  - Multiple VRRP groups exist on the device.
  - A short sending interval is set.

Procedure

1. Enter system view.

   system-view
2. Enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

   vrrp send-gratuitous-arp [**interval** *interval*]

   By default, periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Configuring a subordinate IPv4 VRRP group to follow a master IPv4 VRRP group

About master and subordinate IPv4 VRRP groups

Each VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate VRRP group to follow a master VRRP group.

A master VRRP group determines the device role through exchanging VRRP packets among member devices. A VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Restrictions and guidelines

- To ensure the master router election, configure the settings such as the router priority, preemptive mode, and tracking function for the master IPv4 VRRP group. The settings are not required for subordinate IPv4 VRRP groups.
- You can configure a subordinate VRRP group to follow a master VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv4 VRRP group cannot be both a master group and a subordinate group.
- An IPv4 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master group.
- If an IPv4 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.
- A subordinate IPv4 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of gratuitous ARP packets for IPv4 VRRP by using the **vrrp send-gratuitous-arp** command.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Configure an IPv4 VRRP group as a master group and assign a name to it.

   vrrp vrid *virtual-router-id* **name** *name*

   By default, an IPv4 VRRP group does not act as a master group.
4. Return to system view.

   quit
5. Enter interface view.

   interface *interface-type interface-number*
6. Configure an IPv4 VRRP group to follow a master group.

   vrrp vrid *virtual-router-id* **follow** *name*

   By default, an IPv4 VRRP group does not follow a master VRRP group.

Enabling SNMP notifications for VRRP

About SNMP notifications for VRRP

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Procedure

1. Enter system view.

   system-view
2. Enable SNMP notifications for VRRP.

   snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

   By default, SNMP notifications for VRRP are enabled.

Display and maintenance commands for IPv4 VRRP

Execute **display** commands in any view and the **reset** command in user view.

Task	Command
Display states of IPv4 VRRP groups.	**display vrrp** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]
Display master-to-subordinate IPv4 VRRP group bindings.	**display vrrp binding** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]
Display statistics for IPv4 VRRP groups.	**display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]
Clear statistics for IPv4 VRRP groups.	**reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Configuring IPv6 VRRP

Restrictions and guidelines: IPv6 VRRP configuration

- IPv6 VRRP does not take effect on member ports of aggregation groups.
- Configuration on the routers in an IPv6 VRRP group must be consistent.

IPv6 VRRP tasks at a glance

To configure IPv6 VRRP, perform the following tasks:

1. Specifying an IPv6 VRRP operating mode
2. Configuring an IPv6 VRRP group
3. (Optional.) Configuring VF tracking

   This configuration takes effect only in VRRP load balancing mode.

4. (Optional.) Configuring IPv6 VRRP packet attributes
5. (Optional.) Enabling periodic sending of ND packets for IPv6 VRRP
6. (Optional.) Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

Specifying an IPv6 VRRP operating mode

Restrictions and guidelines

After the IPv6 VRRP operating mode is specified on a router, all IPv6 VRRP groups on the router operate in the specified operating mode.

Procedure

1. Enter system view.

   `system-view`
2. Specify an IPv6 VRRP operating mode.
   - Specify the standard mode.
   - **`undo vrrp ipv6 mode`**
   - Specify the load balancing mode.
   - **`vrrp ipv6 mode load-balance`**

   By default, VRRP operates in standard mode.

Configuring an IPv6 VRRP group

About IPv6 VRRP group

A VRRP group can work correctly after you create it and assign a minimum of one virtual IPv6 address for it. You can configure multiple virtual IPv6 addresses for the VRRP group on an interface that connects to multiple subnets for router backup.

If you disable an IPv6 VRRP group, the VRRP group enters initialized state, and the existing configuration on the VRRP group remains unchanged. You can modify the configuration of the VRRP group. The modification takes effect when you enable the VRRP group again.

Restrictions and guidelines

Item	Remarks
VLAN interface	Do not create VRRP groups on the VLAN interface of a super VLAN. Otherwise, network performance might be adversely affected. For information about the super VLAN feature, see *Layer 2—LAN Switching Configuration Guide*.
Maximum number of VRRP groups and virtual IPv6 addresses	In VRRP load balancing mode, the device supports a maximum of *MaxVRNum/N* VRRP groups. *MaxVRNum* refers to the maximum number of VRRP groups supported by the device in VRRP standard mode. *N* refers to the number of devices in the VRRP group.
Virtual IPv6 address	In load balancing mode, the virtual IPv6 address of a VRRP group cannot be the same as the IPv6 address of any interfaces in the VRRP group. No IP address owner can exist in a VRRP group. An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function. For hosts in the subnet to access external networks, as a best practice, configure the following addresses in the same subnet: • Virtual IPv6 address of an IPv6 VRRP group.

Item	Remarks
	• Downlink interface IPv6 addresses of the VRRP group members.
IP address owner	On an IP address owner, as a best practice, do not use the **ospfv3 area** command to enable OSPF on the interface owning the virtual IPv6 address of the VRRP group. For more information about the **ospfv3 area** command, see *Layer 3—IP Routing Command Reference*. Removal of the VRRP group on the IP address owner causes IP address collision. To avoid the collision, change the IPv6 address of the interface on the IP address owner before you remove the VRRP group from the interface. The running priority of an IP address owner is always 255, and you do not need to configure it. An IP address owner always operates in preemptive mode. If you configure the **vrrp ipv6 vrid track priority reduced** or **vrrp ipv6 vrid track switchover** command on an IP address owner, the configuration does not take effect until the router becomes a non-IP address owner.
VRRP association with a track entry	When the track entry changes from Negative to Positive or Notready, the router automatically restores its priority or the failed master router becomes the master again.

Creating a VRRP group and assign a virtual IPv6 address

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Create a VRRP group and assign a virtual IPv6 address, which is a link-local address.

   vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* **link-local**

   The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address. It must be the last address you remove. Only one link-local address is allowed in a VRRP group.

Configuring an IPv6 VRRP group

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Assign a virtual IPv6 address, which is a global unicast address.

   vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address*

   By default, no global unicast address is assigned to an IPv6 VRRP group.
4. Set the priority of the router in the VRRP group.

   vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

   The default setting is 100.
5. Enable the preemptive mode for the router in a VRRP group and set the preemption delay time.

   vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

   By default, the router in a VRRP group operates in preemptive mode and the preemption delay time is 0 centiseconds, which means an immediate preemption.

6. Associate a VRRP group with a track entry.

   vrrp ipv6 vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ipv6-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

   By default, a VRRP group is not associated with any track entries.

Disabling an IPv6 VRRP group

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Disable an IPv6 VRRP group.

   vrrp ipv6 vrid *virtual-router-id* **shutdown**

   By default, an IPv6 VRRP group is enabled.

Configuring VF tracking

About VF tracking

You can configure VF tracking in both standard mode and load balancing mode, but the function takes effect only in load balancing mode.

In load balancing mode, you can configure the VFs in a VRRP group to monitor a track entry. When the state of the track entry transits to Negative, the weights of all VFs in the VRRP group on the router decrease by a specific value. When the state of the track entry transits to Positive or Notready, the original weights of the VFs restore.

Restrictions and guidelines

- By default, the weight of a VF is 255, and its lower limit of failure is 10.
- When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Configure the VFs in a VRRP group to monitor a track entry.

   vrrp ipv6 vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ipv6-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

   By default, no track entry is specified.

Configuring IPv6 VRRP packet attributes

Restrictions and guidelines

- The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified

interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a VRRP advertisement before the timer (3 x recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

- A high volume of network traffic might cause a backup to fail to receive VRRP advertisements from the master within the specified time. As a result, an unexpected master switchover occurs. To solve this problem, configure a larger interval.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the IPv6 VRRP advertisement interval.

   vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

   The default setting is 100 centiseconds.

   As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

4. Return to system view.

   quit

5. Set a DSCP value for IPv6 VRRP packets.

   vrrp ipv6 dscp *dscp-value*

   By default, the DSCP value for IPv6 VRRP packets is 56.

   The DSCP value identifies the packet priority during transmission.

Enabling periodic sending of ND packets for IPv6 VRRP

About periodic sending of ND packets for IPv6 VRRP

This feature enables the master router in an IPv6 VRRP group to periodically send ND packets. Then the downstream devices can update the MAC address entry for the virtual MAC address of the IPv6 VRRP group in a timely manner.

Restrictions and guidelines

- This feature takes effect only in VRRP standard mode.
- If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.
- The master sends the first ND packet at a random time in the second half of the set interval after you execute the **vrrp ipv6 send-nd** command. This prevents too many ND packets from being sent at the same time.
- The sending interval for ND packets might be much longer than the set interval when the following conditions are met:
  - Multiple IPv6 VRRP groups exist on the device.
  - A short sending interval is set.

Procedure

1. Enter system view.

   system-view

2. Enable periodic sending of ND packets for IPv6 VRRP.

   vrrp ipv6 send-nd [**interval** *interval*]

By default, periodic sending of ND packets is disabled for IPv6 VRRP.

Configuring a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group

About master and subordinate IPv6 VRRP groups

Each IPv6 VRRP group determines the device role (master or backup) by exchanging VRRP packets among member devices, which might consume excessive bandwidth and CPU resources. To reduce the number of VRRP packets in the network, you can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group.

A master IPv6 VRRP group determines the device role through exchanging VRRP packets among member devices. An IPv6 VRRP group that follows a master group, called a subordinate VRRP group, does not exchange VRRP packets among its member devices. The state of the subordinate VRRP group follows the state of the master group.

Restrictions and guidelines

- To ensure the master router election, configure the settings such as the router priority, preemptive mode, and tracking function for the master IPv6 VRRP group. The settings are not required for subordinate IPv6 VRRP groups.
- You can configure a subordinate IPv6 VRRP group to follow a master IPv6 VRRP group in both VRRP standard and load balancing modes. The configuration takes effect only in VRRP standard mode.
- An IPv6 VRRP group cannot be both a master group and a subordinate group.
- An IPv6 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master IPv6 VRRP group.
- If an IPv6 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.
- A subordinate IPv6 VRRP group does not exchange VRRP packets, which might cause the MAC address entry for its virtual MAC address not to be updated on downstream devices. As a best practice, enable periodic sending of ND packets for IPv6 VRRP by using the **vrrp ipv6 send-nd** command.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Configure an IPv6 VRRP group as a master group and assign a name to it.

   vrrp ipv6 vrid *virtual-router-id* **name** *name*

   By default, an IPv6 VRRP group does not act as a master group.
4. Return to system view.

   quit
5. Enter interface view.

   interface *interface-type interface-number*
6. Configure an IPv6 VRRP group to follow a master group.

   vrrp ipv6 vrid *virtual-router-id* **follow** *name*

   By default, an IPv6 VRRP group does not follow a master VRRP group.

Display and maintenance commands for IPv6 VRRP

Execute **display** commands in any view and the **reset** command in user view.

Task	Command
Display the states of IPv6 VRRP groups.	**display vrrp ipv6** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]
Display master-to-subordinate IPv6 VRRP group bindings.	**display vrrp ipv6 binding** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]
Display statistics for IPv6 VRRP groups.	**display vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]
Clear statistics for IPv6 VRRP groups.	**reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

IPv4 VRRP configuration examples

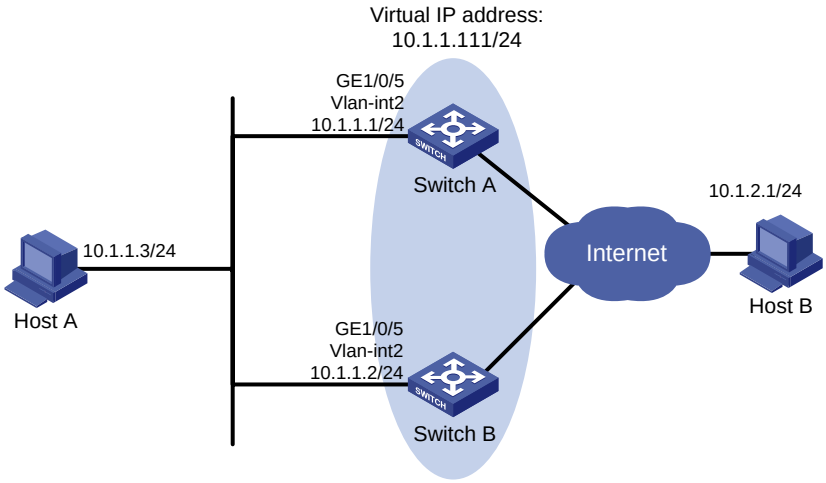
Example: Configuring a single VRRP group

Network configuration

As shown in Figure 9, Switch A and Switch B form a VRRP group. They use the virtual IP address 10.1.1.111/24 to provide gateway service for the subnet where Host A resides.

Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

Figure 9 Network diagram



Procedure

1. Configure Switch A:

   # Configure VLAN 2.

   ```
   <SwitchA> system-view
   ```

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

2. Configure Switch B:

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-Vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.0
```

Create VRRP group 1 on VLAN-interface 2, and set its virtual IP address to 10.1.1.111.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

Set the priority of Router B to 100 in VRRP group 1.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 100
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

Verifying the configuration

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Master
     Config Pri       : 110               Running Pri  : 110
     Preempt Mode     : Yes               Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

```
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Backup
     Config Pri       : 100                  Running Pri  : 100
     Preempt Mode     : Yes                  Delay Time   : 5000
     Become Master    : 401ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Master IP        : 10.1.1.1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 100                  Running Pri  : 100
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.2
```

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 110                  Running Pri  : 110
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
```

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

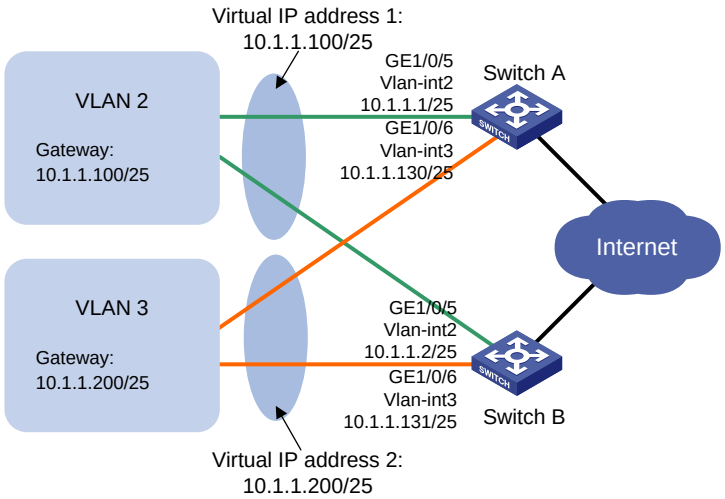
Example: Configuring multiple VRRP groups

Network configuration

As shown in Figure 10, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IP address 10.1.1.100/25 to provide gateway service for hosts in VLAN 2, and VRRP group 2 uses the virtual IP address 10.1.1.200/25 to provide gateway service for hosts in VLAN 3.

Assign a higher priority to Switch A than Switch B in VRRP group 1, but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.

Figure 10 Network diagram



Procedure

1. Configure Switch A:

   # Configure VLAN 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.128
   ```

   # Create VRRP group 1, and set its virtual IP address to 10.1.1.100.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
   ```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.

   ```
   [SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
   [SwitchA-Vlan-interface2] quit
   ```

   # Configure VLAN 3.

   ```
   [SwitchA] vlan 3
   [SwitchA-vlan3] port gigabitethernet 1/0/6
   [SwitchA-vlan3] quit
   [SwitchA] interface vlan-interface 3
   ```

```
[SwitchA-Vlan-interface3] ip address 10.1.1.130 255.255.255.128
```

Create VRRP group 2, and set its virtual IP address to 10.1.1.200.

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
```

2. Configure Switch B:

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.128
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.100.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
[SwitchB-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 10.1.1.131 255.255.255.128
```

Create VRRP group 2, and set its virtual IP address to 10.1.1.200.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
```

Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.

```
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

Verifying the configuration

Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Master
     Config Pri       : 110               Running Pri  : 110
     Preempt Mode     : Yes               Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 10.1.1.100
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1

   Interface Vlan-interface3
     VRID             : 2                 Adver Timer  : 100
     Admin Status     : Up                State        : Backup
     Config Pri       : 100               Running Pri  : 100
     Preempt Mode     : Yes               Delay Time   : 0
     Become Master    : 203ms left
```

```
    Auth Type         : None
    Virtual IP        : 10.1.1.200
    Master IP         : 10.1.1.131
```

Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 0
     Become Master     : 211ms left
     Auth Type         : None
     Virtual IP        : 10.1.1.100
     Master IP         : 10.1.1.1

   Interface Vlan-interface3
     VRID              : 2                 Adver Timer   : 100
     Admin Status      : Up                State         : Master
     Config Pri        : 110               Running Pri   : 110
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : None
     Virtual IP        : 10.1.1.200
     Virtual MAC       : 0000-5e00-0102
     Master IP         : 10.1.1.131
```

The output shows the following information:

- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 10.1.1.100/25.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 10.1.1.200/25.

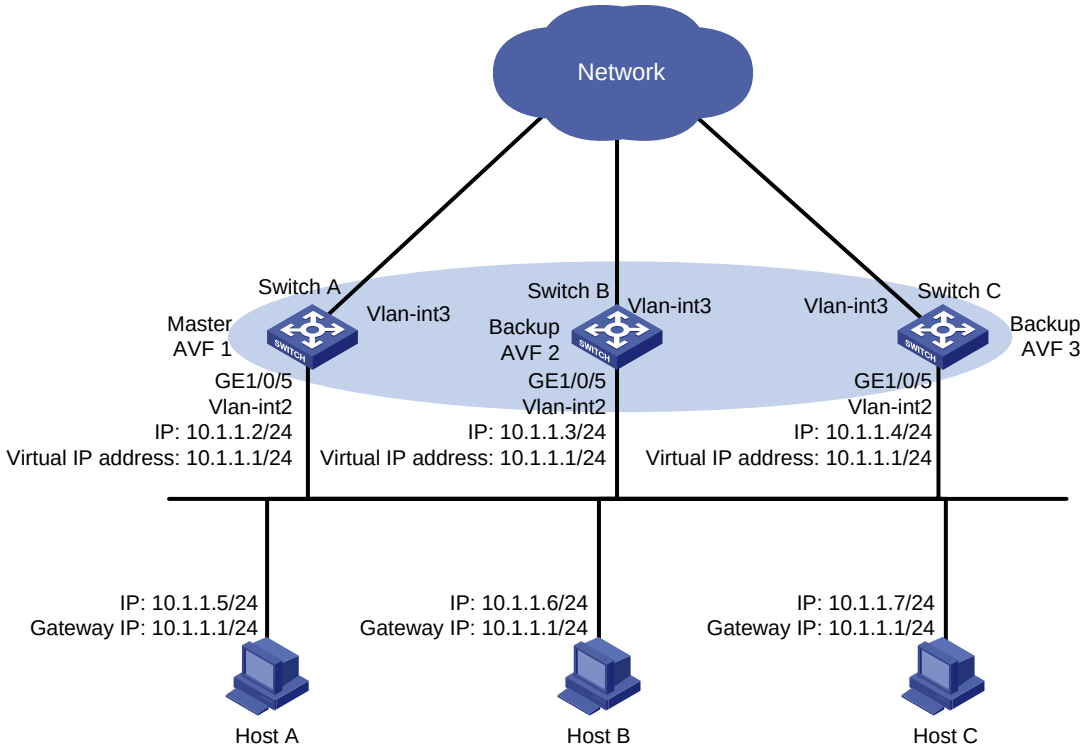
Example: Configuring VRRP load balancing

Network configuration

As shown in Figure 11, Switch A, Switch B, and Switch C form a load-balanced VRRP group. They use the virtual IP address 10.1.1.1/24 to provide gateway service for subnet 10.1.1.0/24.

Configure VFs on Switch A, Switch B, and Switch C to monitor their respective VLAN-interface 3. When the interface on any one of them fails, the weights of the VFs on the problematic switch decrease so another AVF can take over.

Figure 11 Network diagram



Procedure

1. Configure Switch A:

Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchA] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.2 24
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 120
```

Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[SwitchA-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchA] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

2. Configure Switch B:

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.3 24
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[SwitchB-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchB] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

3. Configure Switch C:

Configure VLAN 2.

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 10.1.1.4 24
[SwitchC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[SwitchC-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchC] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 250
```

Verifying the configuration

Verify that Host A can ping the external network. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 120                  Running Pri  : 120
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.1
     Member IP List   : 10.1.1.2 (Local, Master)
                        10.1.1.3 (Backup)
                        10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
```

```
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1                    Adver Timer  : 100
     Admin Status      : Up                   State        : Backup
     Config Pri        : 110                  Running Pri  : 110
     Preempt Mode      : Yes                  Delay Time   : 5000
     Become Master     : 410ms left
     Auth Type         : None
     Virtual IP        : 10.1.1.1
     Member IP List    : 10.1.1.3 (Local, Backup)
                         10.1.1.2 (Master)
                         10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State           : Listening
     Virtual MAC     : 000f-e2ff-0011 (Learnt)
     Owner ID        : 0000-5e01-1101
     Priority        : 127
     Active          : 10.1.1.2
    Forwarder 02
     State           : Active
     Virtual MAC     : 000f-e2ff-0012 (Owner)
     Owner ID        : 0000-5e01-1103
     Priority        : 255
     Active          : local
    Forwarder 03
     State           : Listening
     Virtual MAC     : 000f-e2ff-0013 (Learnt)
     Owner ID        : 0000-5e01-1105
     Priority        : 127
     Active          : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object    : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1                    Adver Timer  : 100
     Admin Status      : Up                   State        : Backup
     Config Pri        : 100                  Running Pri  : 100
     Preempt Mode      : Yes                  Delay Time   : 5000
     Become Master     : 401ms left
     Auth Type         : None
     Virtual IP        : 10.1.1.1
```

```
    Member IP List   : 10.1.1.4 (Local, Backup)
                       10.1.1.2 (Master)
                       10.1.1.3 (Backup)
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Listening
    Virtual MAC    : 000f-e2ff-0011 (Learnt)
    Owner ID       : 0000-5e01-1101
    Priority       : 127
    Active         : 10.1.1.2
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

Disconnect the link of VLAN-interface 3 on Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                   Adver Timer  : 100
     Admin Status     : Up                  State        : Master
     Config Pri       : 120                 Running Pri  : 120
     Preempt Mode     : Yes                 Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.1
     Member IP List   : 10.1.1.2 (Local, Master)
                        10.1.1.3 (Backup)
                        10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
```

```
    State           : Initialize
    Virtual MAC     : 000f-e2ff-0011 (Owner)
    Owner ID        : 0000-5e01-1101
    Priority        : 0
    Active          : 10.1.1.4
  Forwarder 02
    State           : Initialize
    Virtual MAC     : 000f-e2ff-0012 (Learnt)
    Owner ID        : 0000-5e01-1103
    Priority        : 0
    Active          : 10.1.1.3
  Forwarder 03
    State           : Initialize
    Virtual MAC     : 000f-e2ff-0013 (Learnt)
    Owner ID        : 0000-5e01-1105
    Priority        : 0
    Active          : 10.1.1.4
 Forwarder Weight Track Information:
    Track Object    : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                   Adver Timer  : 100
     Admin Status     : Up                  State        : Backup
     Config Pri       : 100                 Running Pri  : 100
     Preempt Mode     : Yes                 Delay Time   : 5000
     Become Master    : 401ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.1
     Member IP List   : 10.1.1.4 (Local, Backup)
                        10.1.1.2 (Master)
                        10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State           : Active
     Virtual MAC     : 000f-e2ff-0011 (Take Over)
     Owner ID        : 0000-5e01-1101
     Priority        : 85
     Active          : local
    Forwarder 02
     State           : Listening
     Virtual MAC     : 000f-e2ff-0012 (Learnt)
     Owner ID        : 0000-5e01-1103
```

```
    Priority       : 85
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Switch C becomes the AVF to forward traffic.

When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                   Adver Timer  : 100
     Admin Status     : Up                  State        : Backup
     Config Pri       : 100                 Running Pri  : 100
     Preempt Mode     : Yes                 Delay Time   : 5000
     Become Master    : 402ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.1
     Member IP List   : 10.1.1.4 (Local, Backup)
                        10.1.1.2 (Master)
                        10.1.1.3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-0011 is removed. The VF no longer forwards the packets destined for the MAC address.

When Switch A fails, display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer   : 100
     Admin Status     : Up                   State         : Master
     Config Pri       : 110                  Running Pri   : 110
     Preempt Mode     : Yes                  Delay Time    : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.1
     Member IP List   : 10.1.1.3 (Local, Master)
                        10.1.1.4 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows the following information:

- When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
- The VF for virtual MAC address 000f-e2ff-0011 is removed.

IPv6 VRRP configuration examples

Example: Configuring a single VRRP group

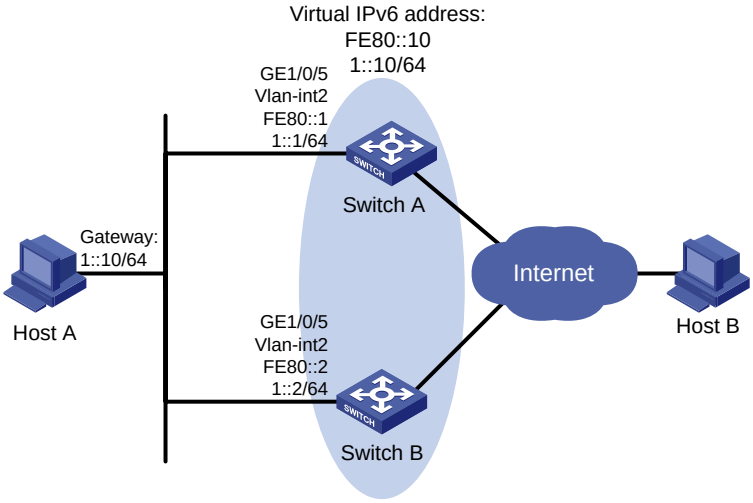
Network configuration

As shown in Figure 12, Switch A and Switch B form a VRRP group. They use the virtual IP addresses 1::10/64 and FE80::10 to provide gateway service for the subnet where Host A resides.

Host A learns 1::10/64 as its default gateway from RA messages sent by the switches.

Switch A operates as the master to forward packets from Host A to Host B. When Switch A fails, Switch B takes over to forward packets for Host A.

Figure 12 Network diagram



Procedure

1. Configure Switch A:

   # Configure VLAN 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   ```

   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   ```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
   ```

   # Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

   ```
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
   ```

   # Enable Switch A to send RA messages, so Host A can learn the default gateway address.

   ```
   [SwitchA-Vlan-interface2] undo ipv6 nd ra halt
   ```

2. Configure Switch B:

   # Configure VLAN 2.

   ```
   <SwitchB> system-view
   [SwitchB] vlan 2
   [SwitchB-vlan2] port gigabitethernet 1/0/5
   [SwitchB-vlan2] quit
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
   [SwitchB-Vlan-interface2] ipv6 address 1::2 64
   ```

   # Create VRRP group 1 and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Enable Switch B to send RA messages, so Host A can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

Verifying the configuration

Ping Host B from Host A. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::1
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode        : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 5000
     Become Master    : 403ms left
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Master IP        : FE80::1
```

The output shows that Switch A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

Disconnect the link between Host A and Switch A, and verify that Host A can still ping Host B. (Details not shown.)

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
```

```
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1                   Adver Timer   : 100
     Admin Status      : Up                  State         : Master
     Config Pri        : 100                 Running Pri   : 100
     Preempt Mode      : Yes                 Delay Time    : 5000
     Auth Type         : None
     Virtual IP        : FE80::10
                         1::10
     Virtual MAC       : 0000-5e00-0201
     Master IP         : FE80::2
```

The output shows that when Switch A fails, Switch B takes over to forward packets from Host A to Host B.

Recover the link between Host A and Switch A, and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1                   Adver Timer   : 100
     Admin Status      : Up                  State         : Master
     Config Pri        : 110                 Running Pri   : 110
     Preempt Mode      : Yes                 Delay Time    : 5000
     Auth Type         : None
     Virtual IP        : FE80::10
                         1::10
     Virtual MAC       : 0000-5e00-0201
     Master IP         : FE80::1
```

The output shows that after Switch A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

Example: Configuring multiple VRRP groups

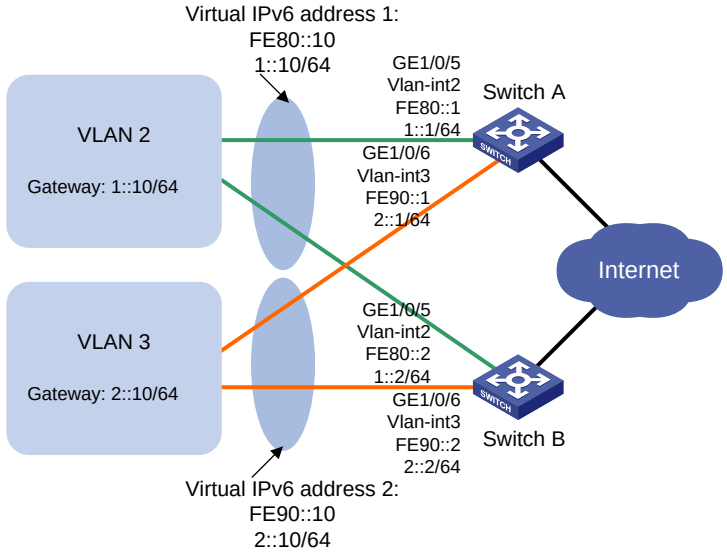
Network configuration

As shown in Figure 13, Switch A and Switch B form two VRRP groups. VRRP group 1 uses the virtual IPv6 addresses 1::10/64 and FE80::10 to provide gateway service for hosts in VLAN 2. VRRP group 2 uses the virtual IPv6 addresses 2::10/64 and FE90::10 to provide gateway service for hosts in VLAN 3.

From RA messages sent by the switches, hosts in VLAN 2 learn 1::10/64 as their default gateway. Hosts in VLAN 3 learn 2::10/64 as their default gateway.

Assign Switch A a higher priority than Switch B in VRRP group 1 but a lower priority in VRRP group 2. Traffic from VLAN 2 and VLAN 3 can then be distributed between the two switches. When one of the switches fails, the healthy switch provides gateway service for both VLANs.

Figure 13 Network diagram



Procedure

1. Configure Switch A:

   # Configure VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 to 1::10.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

   # Assign Switch A a higher priority than Switch B in VRRP group 1, so Switch A can become the master in the group.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

   # Enable Switch A to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
```

   # Configure VLAN 3.

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64
```

   # Create VRRP group 2, and set its virtual IPv6 addresses to FE90::10 and 2::10.

```
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

Enable Switch A to send RA messages, so hosts in VLAN 3 can learn the default gateway address.

```
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

2. Configure Switch B:

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Enable Switch B to send RA messages, so hosts in VLAN 2 can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
```

Configure VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
[SwitchB-Vlan-interface3] ipv6 address 2::2 64
```

Create VRRP group 2, and set its virtual IPv6 addresses to FE90::10 and 2::10.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

Assign Switch B a higher priority than Switch A in VRRP group 2, so Switch B can become the master in the group.

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
```

Enable Switch B to send RA messages, so hosts in VLAN 3 can learn the default gateway address.

```
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

Verifying the configuration

Display detailed information about the VRRP groups on Switch A.

```
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID              : 1                 Adver Timer  : 100
     Admin Status      : Up                State        : Master
     Config Pri        : 110               Running Pri  : 110
     Preempt Mode      : Yes               Delay Time   : 0
     Auth Type         : None
     Virtual IP        : FE80::10
                         1::10
```

```
    Virtual MAC      : 0000-5e00-0201
    Master IP        : FE80::1

  Interface Vlan-interface3
    VRID             : 2                    Adver Timer  : 100
    Admin Status     : Up                   State        : Backup
    Config Pri       : 100                  Running Pri  : 100
    Preempt Mode     : Yes                  Delay Time   : 0
    Become Master    : 402ms left
    Auth Type        : None
    Virtual IP       : FE90::10
                       2::10
    Master IP        : FE90::2
```

Display detailed information about the VRRP groups on Switch B.

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Backup
     Config Pri       : 100                  Running Pri  : 100
     Preempt Mode     : Yes                  Delay Time   : 0
     Become Master    : 401ms left
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Master IP        : FE80::1

   Interface Vlan-interface3
     VRID             : 2                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 110                  Running Pri  : 110
     Preempt Mode     : Yes                  Delay Time   : 0
     Auth Type        : None
     Virtual IP       : FE90::10
                        2::10
     Virtual MAC      : 0000-5e00-0202
     Master IP        : FE90::2
```

The output shows the following information:

- Switch A is operating as the master in VRRP group 1 to forward Internet traffic for hosts that use the default gateway 1::10/64.
- Switch B is operating as the master in VRRP group 2 to forward Internet traffic for hosts that use the default gateway 2::10/64.

Example: Configuring VRRP load balancing

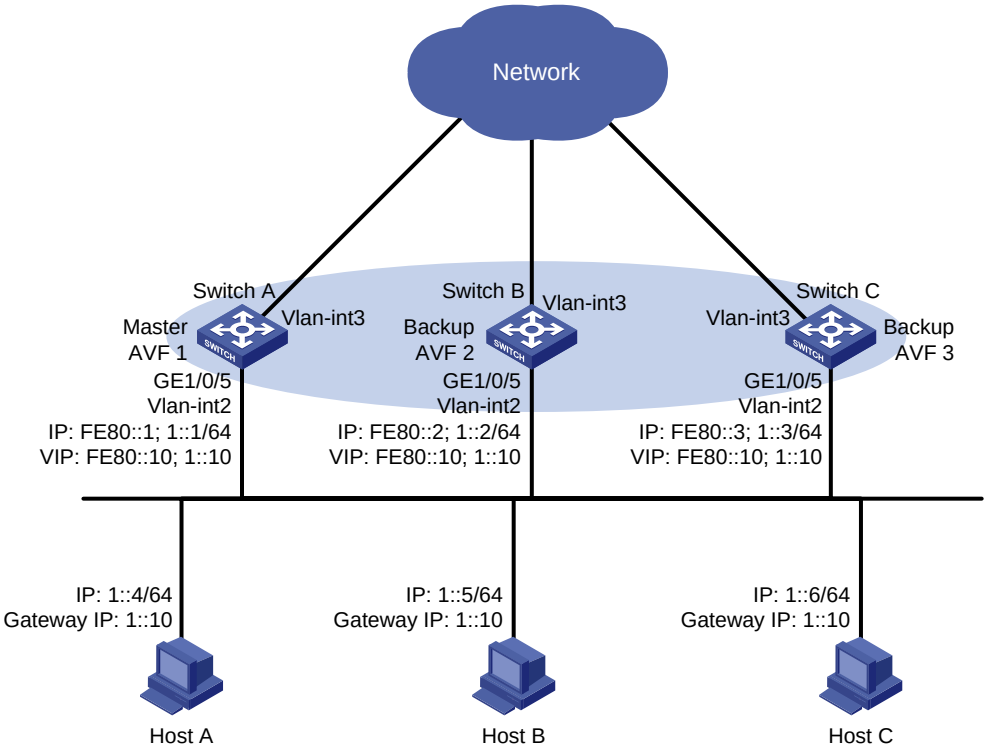
Network configuration

As shown in Figure 14, Switch A, Switch B, and Switch C form a load balanced VRRP group. They use the virtual IPv6 addresses FE80::10 and 1::10 to provide gateway service for subnet 1::/64.

Hosts on subnet 1::/64 learn 1::10 as their default gateway from RA messages sent by the switches.

Configure VFs on Switch A, Switch B, or Switch C to monitor their respective VLAN-interface 3. When the interface on any of them fails, the weights of the VFs on the problematic switch decrease so another AVF can take over.

Figure 14 Network diagram



Procedure

1. Configure Switch A:

   # Configure VLAN 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/5
   [SwitchA-vlan2] quit
   ```

   # Configure VRRP to operate in load balancing mode.

   ```
   [SwitchA] vrrp ipv6 mode load-balance
   ```

   # Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
   [SwitchA-Vlan-interface2] ipv6 address 1::1 64
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
   [SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
   ```

Assign Switch A the highest priority in VRRP group 1, so Switch A can become the master.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120
```

Configure Switch A to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Enable Switch A to send RA messages, so hosts on subnet 1::/64 can learn the default gateway address.

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchA] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250
```

2. Configure Switch B:

Configure VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchB] vrrp ipv6 mode load-balance
```

Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Assign Switch B a higher priority than Switch C in VRRP group 1, so Switch B can become the master when Switch A fails.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

Configure Switch B to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Enable Switch B to send RA messages so hosts on subnet 1::/64 can learn the default gateway address.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchB] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250
```

3. Configure Switch C:

Configure VLAN 2.

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/5
[SwitchC-vlan2] quit
```

Configure VRRP to operate in load balancing mode.

```
[SwitchC] vrrp ipv6 mode load-balance
```

Create VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ipv6 address fe80::3 link-local
[SwitchC-Vlan-interface2] ipv6 address 1::3 64
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure Switch C to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Enable Switch C to send RA messages, so the hosts on the subnet 1::/64 can learn the default gateway address.

```
[SwitchC-Vlan-interface2] undo ipv6 nd ra halt
[SwitchC-Vlan-interface2] quit
```

Create track entry 1 to monitor the upstream link status of VLAN-interface 3. When the upstream link fails, the track entry transits to Negative.

```
[SwitchC] track 1 interface vlan-interface 3
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 250
```

Verifying the configuration

Verify that Host A can ping the external network. (Details not shown.)

Display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 120                  Running Pri  : 120
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Member IP List   : FE80::1 (Local, Master)
                        FE80::2 (Backup)
                        FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
```

```
    Forwarder 01
      State            : Active
      Virtual MAC      : 000f-e2ff-4011 (Owner)
      Owner ID         : 0000-5e01-1101
      Priority         : 255
      Active           : local
    Forwarder 02
      State            : Listening
      Virtual MAC      : 000f-e2ff-4012 (Learnt)
      Owner ID         : 0000-5e01-1103
      Priority         : 127
      Active           : FE80::2
    Forwarder 03
      State            : Listening
      Virtual MAC      : 000f-e2ff-4013 (Learnt)
      Owner ID         : 0000-5e01-1105
      Priority         : 127
      Active           : FE80::3
  Forwarder Weight Track Information:
    Track Object    : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Backup
     Config Pri       : 110                  Running Pri  : 110
     Preempt Mode     : Yes                  Delay Time   : 5000
     Become Master    : 401ms left
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Member IP List   : FE80::2 (Local, Backup)
                        FE80::1 (Master)
                        FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State            : Listening
     Virtual MAC      : 000f-e2ff-4011 (Learnt)
     Owner ID         : 0000-5e01-1101
     Priority         : 127
     Active           : FE80::1
    Forwarder 02
     State            : Active
```

```
    Virtual MAC    : 000f-e2ff-4012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
  Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-4013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                   Adver Timer  : 100
     Admin Status     : Up                  State        : Backup
     Config Pri       : 100                 Running Pri  : 100
     Preempt Mode     : Yes                 Delay Time   : 5000
     Become Master    : 402ms left
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Member IP List   : FE80::3 (Local, Backup)
                        FE80::1 (Master)
                        FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
   Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-4011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : FE80::1
   Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
   Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
```

```
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that Switch A is the master in VRRP group 1, and each of the three switches has one AVF and two LVFs.

Disconnect the link of VLAN-interface 3 on Switch A and display detailed information about VRRP group 1 on Switch A.

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 120                  Running Pri  : 120
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Member IP List   : FE80::1 (Local, Master)
                        FE80::2 (Backup)
                        FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
    Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : FE80::3
    Forwarder 02
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 0
     Active         : FE80::2
    Forwarder 03
     State          : Initialize
     Virtual MAC    : 000f-e2ff-4013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 0
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
```

```
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Backup
     Config Pri       : 100                  Running Pri  : 100
     Preempt Mode     : Yes                  Delay Time   : 5000
     Become Master    : 410ms left
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Member IP List   : FE80::3 (Local, Backup)
                        FE80::1 (Master)
                        FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-4011 (Take Over)
     Owner ID       : 0000-5e01-1101
     Priority       : 85
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-4012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 85
     Active         : FE80::2
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-4013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when VLAN-interface 3 on Switch A fails, the weights of the VFs on Switch A drop below the lower limit of failure. All VFs on Switch A transit to the Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-4011 on Switch C becomes the AVF to forward traffic.

When the timeout timer (about 1800 seconds) expires, display detailed information about VRRP group 1 on Switch C.

```
[SwitchC-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
```

```
    VRID              : 1                    Adver Timer  : 100
    Admin Status      : Up                   State        : Backup
    Config Pri        : 100                  Running Pri  : 100
    Preempt Mode      : Yes                  Delay Time   : 5000
    Become Master     : 400ms left
    Auth Type         : None
    Virtual IP        : FE80::10
                        1::10
    Member IP List    : FE80::3 (Local, Backup)
                        FE80::1 (Master)
                        FE80::2 (Backup)
  Forwarder Information: 2 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 02
    State           : Listening
    Virtual MAC     : 000f-e2ff-4012 (Learnt)
    Owner ID        : 0000-5e01-1103
    Priority        : 127
    Active          : FE80::2
   Forwarder 03
    State           : Active
    Virtual MAC     : 000f-e2ff-4013 (Owner)
    Owner ID        : 0000-5e01-1105
    Priority        : 255
    Active          : local
  Forwarder Weight Track Information:
    Track Object    : 1          State : Positive   Weight Reduced : 250
```

The output shows that when the timeout timer expires, the VF for virtual MAC address 000f-e2ff-4011 is removed. The VF no longer forwards the packets destined for the MAC address.

When Switch A fails, display detailed information about VRRP group 1 on Switch B.

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1                    Adver Timer  : 100
     Admin Status      : Up                   State        : Master
     Config Pri        : 110                  Running Pri  : 110
     Preempt Mode      : Yes                  Delay Time   : 5000
     Auth Type         : None
     Virtual IP        : FE80::10
                         1::10
     Member IP List    : FE80::2 (Local, Master)
                         FE80::3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
```

```
Forwarder 02
 State           : Active
 Virtual MAC     : 000f-e2ff-4012 (Owner)
 Owner ID        : 0000-5e01-1103
 Priority        : 255
 Active          : local
Forwarder 03
 State           : Listening
 Virtual MAC     : 000f-e2ff-4013 (Learnt)
 Owner ID        : 0000-5e01-1105
 Priority        : 127
 Active          : FE80::3
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows the following information:

- When Switch A fails, Switch B becomes the master because it has a higher priority than Switch C.
- The VF for virtual MAC address 000f-e2ff-4011 is removed.

Troubleshooting VRRP

An error prompt is displayed

Symptom

An error prompt "The virtual router detected a VRRP configuration error." is displayed during configuration.

Analysis

This symptom is probably caused by the following reasons:

- The VRRP advertisement interval in the packet is not the same as that for the current VRRP group (in VRRPv2 only).
- The number of virtual IP addresses in the packet is not the same as that for the current VRRP group.
- The virtual IP address list is not the same as that for the current VRRP group.
- A device in the VRRP group receives illegitimate VRRP packets. For example, the IP address owner receives a VRRP packet with the priority 255.

Solution

To resolve the problem:

1. Modify the configuration on routers in VRRP groups to ensure consistent configuration.
2. Take fault location and anti-attack measures to eliminate potential threats.
3. If the problem persists, contact Hewlett Packard Enterprise Support.

Multiple masters appear in a VRRP group

Symptom

Multiple masters appear in a VRRP group.

Analysis

It is normal for a VRRP group to have multiple masters for a short time, and this situation requires no manual intervention.

If multiple masters coexist for a longer period, check for the following conditions:

- The masters cannot receive advertisements from each other.
- The received advertisements are illegitimate.

Solution

To resolve the problem:

1. Ping between these masters:
   - If the ping operation fails, examine network connectivity.
   - If the ping operation succeeds, check for configuration inconsistencies in the number of virtual IP addresses, virtual IP addresses, and authentication. For IPv4 VRRP, also make sure the same version of VRRP is configured on all routers in the VRRP group. For VRRPv2, make sure the same VRRP advertisement interval is configured on the routers in the VRRP group.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

Fast VRRP state flapping

Symptom

Fast VRRP state flapping occurs.

Analysis

The VRRP advertisement interval is set too short.

Solution

To resolve the problem:

1. Increase the interval for sending VRRP advertisements or introduce a preemption delay.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

IPv4 VRRP commands

VRRP does not take effect on member ports of aggregation groups.

display vrrp

Use **display vrrp** to display the states of IPv4 VRRP groups.

Syntax

display vrrp [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv4 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv4 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv4 VRRP groups.

If only an interface is specified, this command displays the states of all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays the states of the specified IPv4 VRRP group on the specified interface.

Examples

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     100     Simple   1.1.1.1
```

Table 1 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets. This field is displayed only after you configure the **vrrp send-gratuitous-arp** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.

Field	Description
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Gratuitous ARP sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                   Adver Timer  : 100
     Admin Status     : Up                  State        : Master
     Config Pri       : 150                 Running Pri  : 150
     Preempt Mode     : Yes                 Delay Time   : 5
     Auth Type        : Simple              Key          : ******
     Virtual IP       : 1.1.1.1
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 1.1.1.2
     Config Role      : Master
     Name             : abc
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 50

   Interface Vlan-interface2
     VRID             : 2                   Adver Timer  : 100
     Admin Status     : Up                  State        : Backup
     Config Pri       : 80                  Running Pri  : 80
     Preempt Mode     : Yes                 Delay Time   : 0
     Become Master    : 2370ms left
     Auth Type        : None
     Virtual IP       : 1.1.1.11
     Virtual MAC      : 0000-5e00-0102
     Master IP        : 1.1.1.12

   Interface Vlan-interface2
     VRID             : 3                   Adver Timer : 100
     Admin Status     : Up                  State       : Master
     Config Pri       : 100                 Running Pri : 100
     Preempt Mode     : Yes                 Delay Time  : 0
     Auth Type        : None
     Pkt Sending Mode : v2-only
     Virtual IP       : 1.1.1.10
     Virtual MAC      : 0000-5e00-0103
```

```
Master IP         : 1.1.1.2
Config Role       : Subordinate
Follow Name       : abc
```

Table 2 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
Gratuitous ARP sending interval	Sending interval for gratuitous ARP packets. This field is displayed only after you configure the **vrrp send-gratuitous-arp** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.
Config Pri	Configured priority of the router, which is configured by using the **vrrp vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Key	Authentication key, which is not displayed if no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Primary IP address of the interface where the master resides.
Config Role	The configured role of the VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the VRRP group. This field is displayed only after you configure the **vrrp vrid name** command.

Field	Description
Follow Name	Name of the master VRRP group that the VRRP group follows. This field is displayed only after you configure the **vrrp vrid follow** command.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry changes to the Negative state.
Switchover	Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master.

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
 Interface          VRID  State        Running Address             Active
                                       Pri
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     1.1.1.1             Local
 -----              VF 1  Active       255     000f-e2ff-0011      Local
```

Table 3 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number) or virtual forwarder (VF) ID.
State	• For a VRRP group, this field indicates the state of the router in the VRRP group, which is **Master**, **Backup**, **Initialize**, or **Inactive**. • For a VF, this field indicates the state of the VF in the VRRP group, which is **Active**, **Listening**, or **Initialize**.
Running Pri	• For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. • For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the track entry's status changes.

Field	Description
Address	• For a VRRP group, this field indicates the virtual IP address of the VRRP group. • For a VF, this field indicates the virtual MAC address of the VF.
Active	• For a VRRP group, this field indicates the IP address of the interface where the master resides. If the current router is the master, this field displays **local**. • For a VF, this field indicates the IP address of the interface where the active virtual forwarder (AVF) resides. If the current VF is the AVF, this field displays **local**.

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 150                 Running Pri  : 150
     Preempt Mode   : Yes                 Delay Time   : 5
     Auth Type      : None
     Virtual IP     : 10.1.1.1
                      10.1.1.2
                      10.1.1.3
     Member IP List : 10.1.1.10 (Local, Master)
                      10.1.1.20 (Backup)
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 50
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.20
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
   Interface Vlan-interface2
     VRID           : 11                  Adver Timer  : 100
```

```
  Admin Status   : Up                   State        : Backup
  Config Pri     : 80                   Running Pri  : 80
  Preempt Mode   : Yes                  Delay Time   : 0
  Become Master  : 2370ms left
  Auth Type      : None
  Virtual IP     : 10.1.1.11
                 : 10.1.1.12
                 : 10.1.1.13
  Member IP List : 10.1.1.10 (Local, Backup)
                   10.1.1.15 (Master)
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-40b1 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : 10.1.1.15
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-40b2 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
```

Table 4 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.
Config Pri	Configured priority of the router, which is configured by using the **vrrp vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.

Field	Description
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type: • **None**—No authentication. • **Simple**—Simple text authentication. • **MD5**—MD5 authentication.
Key	Authentication key, which is not displayed if no authentication is required.
Virtual IP	Virtual IP address list of the VRRP group.
Member IP List	IP addresses of the member devices in the VRRP group: • **Local**—IP address of the local router. • **Master**—IP address of the master. • **Backup**—IP address of the backup.
VRRP Track Information	Track entry which is associated with the VRRP group. This field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry to be monitored.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry changes to the Negative state. This field is displayed only after you configure the **vrrp vrid track** command.
Switchover	Switchover mode. When the status of the associated track entry changes to the Negative state, the backup immediately becomes the master.
Forwarder Information: 2 Forwarders 1 Active	VF information: Two VFs exist, and one is the AVF.
Config Weight	Configured weight of the VF: 255.
Running Weight	Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes.
Forwarder 01	Information about VF 01.
State	VF state: • **Active**. • **Listening**. • **Initialize**.
Virtual MAC	Virtual MAC address of the VF.
Owner ID	Real MAC address of the VF owner.
Priority	VF priority in the range of 1 to 255.

Field	Description
Active	IP address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.
Forwarder Weight Track Configuration	VF weight Track configuration. The field is displayed only after you configure the **vrrp vrid track** command.
Track Object	Track entry that is associated with the VFs. The field is displayed only after you configure the **vrrp vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Weight Reduced	Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative. The field is displayed only after you configure the **vrrp vrid track** command.
Forwarder Switchover Track Information:	VF switchover Track configuration. The field is displayed only after you configure the **vrrp vrid track** command.
Member IP	IP address of a member device. The field is displayed only after you configure the **vrrp vrid track** command.

display vrrp binding

Use **display vrrp binding** to display master-to-subordinate IPv4 VRRP group bindings.

Syntax

display vrrp binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv4 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name *name*: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv4 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master VRRP group, this command displays all master-to-subordinate VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv4 VRRP group bindings.

```
<Sysname> display vrrp binding
IPv4 virtual router binding information:
  Total number of master virtual routers            : 1
  Total number of subordinate virtual routers       : 2
  Interface : Vlan2                    Master VRID : 1
  Name      : a                        Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 4

  Interface : --                       Master VRID : --
  Name      : c                        Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 5
```

Table 5 Command output

Field	Description
Total number of master virtual routers	Total number of master VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate VRRP groups.
Interface	Interface to which the master VRRP group belongs. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master VRRP group. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master VRRP group.
Status	Status of the router in the master VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**. If the master VRRP group does not exist, this field displays two hyphens (**--**).
Subordinate virtual routers	Number of subordinate VRRP groups.
Interface	Interface to which the subordinate VRRP group belongs.
VRID	Virtual router ID of the subordinate VRRP group.

Related commands

vrrp vrid follow

vrrp vrid name

display vrrp statistics

Use **display vrrp statistics** to display statistics for IPv4 VRRP groups.

Syntax

display vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv4 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command displays statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Display statistics for all IPv4 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
 Invalid Pkts Rcvd  :     0          Unexpected Pkts Rcvd         : 0
 IP TTL Errors          : 0          Advertisement Interval Errors : 0
 Invalid Auth Type      : 0          Auth Failures                : 0
 Packet Length Errors   : 0          Auth Type Mismatch           : 0
 Become Master          : 1          Address List Errors          : 0
 Adver Rcvd             : 0          Priority Zero Pkts Rcvd      : 0
 Adver Sent             : 807        Priority Zero Pkts Sent      : 0
IP Owner Conflicts     : 0

 Global statistics
 CheckSum Errors        : 0
 Version Errors         : 0
```

```
 VRID Errors              : 0
```

Display statistics for all IPv4 VRRP groups when VRRP operates in load balancing mode.

```
<Sysname> display vrrp statistics
 Interface               : Vlan-interface2
 VRID                    : 1
 CheckSum Errors         : 0          Version Errors               : 0
 Invalid Pkts Rcvd       : 0          Unexpected Pkts Rcvd         : 0
 IP TTL Errors           : 0          Advertisement Interval Errors : 0
 Invalid Auth Type       : 0          Auth Failures                : 0
 Packet Length Errors    : 0          Auth Type Mismatch           : 0
 Become Master           : 39         Address List Errors          : 0
 Become AVF              : 13         Packet Option Errors         : 0
 Adver Rcvd              : 2562       Priority Zero Pkts Rcvd      : 1
 Adver Sent              : 16373      Priority Zero Pkts Sent      : 49
 Request Rcvd            : 2          Reply Rcvd                   : 10
 Request Sent            : 12         Reply Sent                   : 2
 Release Rcvd            : 0          VF Priority Zero Pkts Rcvd   : 1
 Release Sent            : 0          VF Priority Zero Pkts Sent   : 11
 Redirect Timer Expires  : 1          Time-out Timer Expires       : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Table 6 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
IP TTL Errors	Number of packets with TTL errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.

Field	Description
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Table 7 Command output (in load balancing mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
IP TTL Errors	Number of packets with TTL errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Redirect Timer Expires	Number of times that the redirect timer expired.
Become AVF	Number of times that the VF has been elected as the AVF.
Time-out Timer Expires	Number of times that the time-out timer expired.
Adver Rcvd	Number of received advertisements.
Request Rcvd	Number of received requests.
Adver Sent	Number of sent advertisements.
Request Sent	Number of sent requests.
Reply Rcvd	Number of received replies.

Field	Description
Release Rcvd	Number of received release packets.
Reply Sent	Number of sent replies.
Release Sent	Number of sent release packets.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
VF Priority Zero Pkts Rcvd	Number of received advertisements with the VF priority of 0.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
VF Priority Zero Pkts Sent	Number of sent advertisements with the VF priority of 0.
Packet Option Errors	Number of packet option errors.
Global statistics	Global statistics for all IPv4 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

reset vrrp statistics

reset vrrp statistics

Use **reset vrrp statistics** to clear statistics for IPv4 VRRP groups.

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv4 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv4 VRRP groups on the specified interface.

If both an interface and an IPv4 VRRP group are specified, this command clears statistics for the specified IPv4 VRRP group on the specified interface.

Examples

Clear statistics for all IPv4 VRRP groups on all interfaces.

```
<Sysname> reset vrrp statistics
```

Related commands

display vrrp statistics

snmp-agent trap enable vrrp

Use **snmp-agent trap enable vrrp** to enable SNMP notifications for VRRP.

Use **undo snmp-agent trap enable vrrp** to disable SNMP notifications for VRRP.

Syntax

snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

undo snmp-agent trap enable vrrp [**auth-failure** | **new-master**]

Default

SNMP notifications for VRRP are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Generates notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

new-master: Generates notifications as defined in RFC 2787 when the state of a device in a VRRP group changes from Initialize or Backup to Master.

Usage guidelines

To report critical VRRP events to an NMS, enable SNMP notifications for VRRP. For VRRP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Generate notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable vrrp auth-failure
```

vrrp check-ttl enable

Use **vrrp check-ttl enable** to enable TTL check for IPv4 VRRP packets.

Use **undo vrrp check-ttl enable** to disable TTL check for IPv4 VRRP packets.

Syntax

vrrp check-ttl enable

undo vrrp check-ttl enable

Default

TTL check for IPv4 VRRP packets is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. The VRRP advertisements are multicast in the local subnet and cannot be forwarded by routers, so the TTL value is not changed. When the master sends VRRP advertisements, it sets the TTL value to 255. If you enable TTL check, the backups drop the VRRP advertisements with TTL other than 255, preventing attacks from other subnets.

Devices from different vendors might implement VRRP differently. When the device is interoperating with devices of other vendors, TTL check on VRRP packets might result in unexpected dropping of packets. In this scenario, use the **undo vrrp check-ttl enable** command to disable TTL check on VRRP packets.

Examples

Disable TTL check for IPv4 VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] undo vrrp check-ttl enable
```

vrrp dscp

Use **vrrp dscp** to set a DSCP value for VRRP packets.

Use **undo vrrp dscp** to restore the default.

Syntax

vrrp dscp *dscp-value*

undo vrrp dscp

Default

The DSCP value for VRRP packets is 48.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for VRRP packets.

```
<Sysname> system-view
[Sysname] vrrp dscp 30
```

vrrp mode

Use **vrrp mode** to specify the operating mode for IPv4 VRRP.

Use **undo vrrp mode** to restore the default.

Syntax

vrrp mode load-balance [**version-8**]

undo vrrp mode

Default

IPv4 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

version-8: Specifies the version carried in VRRP packets as 8.

Usage guidelines

After you create IPv4 VRRP groups on the router, you can use this command to modify their operating mode. All IPv4 VRRP groups on the router operate in the specified mode.

The **version-8** keyword takes effect only when the version of IPv4 VRRP configured on the interface is VRRPv2. The **version-8** keyword is required in the following conditions:

- A router running Comware 5 software exists in the VRRP group.

  To display the software version, use the **display version** command.
- All routers in the IPv4 VRRP group are operating in load balancing mode.
- All routers in the IPv4 VRRP group are configured with the version of VRRPv2.

Examples

Specify the load balancing mode for IPv4 VRRP.

```
<Sysname> system-view
[Sysname] vrrp mode load-balance
```

Related commands

display vrrp

vrrp send-gratuitous-arp

Use **vrrp send-gratuitous-arp** to enable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Use **undo vrrp send-gratuitous-arp** to disable periodic sending of gratuitous ARP packets for IPv4 VRRP.

Syntax

vrrp send-gratuitous-arp [**interval** *interval*]

undo vrrp send-gratuitous-arp

Default

Periodic sending of gratuitous ARP packets is disabled for IPv4 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of a VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.

The master sends the first gratuitous ARP packet at a random time in the second half of the set interval after you execute the **vrrp send-gratuitous-arp** command. This prevents too many gratuitous ARP packets from being sent at the same time.

The sending interval for gratuitous ARP packets might be much longer than the set interval when the following conditions are met:

- Multiple VRRP groups exist on the device.
- A short sending interval is set.

Examples

Enable periodic sending of gratuitous ARP packets for IPv4 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
[Sysname] vrrp send-gratuitous-arp interval 200
```

vrrp version

Use **vrrp version** to specify the version of IPv4 VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv3 is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3, where 2 indicates VRRPv2 (described in RFC 3768), and 3 indicates VRRPv3 (described in RFC 5798).

Usage guidelines

The version of VRRP on all routers in an IPv4 VRRP group must be the same.

Examples

Specify VRRPv2 to run on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp version 2
```

vrrp vrid

Use **vrrp vrid** to create an IPv4 VRRP group and assign a virtual IP address to it, or to assign a virtual IP address to an existing IPv4 VRRP group.

Use **undo vrrp vrid** to remove all configurations of an IPv4 VRRP group, or to remove a virtual IP address from an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

Default

No IPv4 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IP address. You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.
- Invalid IP address (for example, 0.0.0.1).

If you do not specify the *virtual-address* argument, the **undo vrrp vrid** command removes all virtual IP addresses from the specified IPv4 VRRP group.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IP addresses to an IPv4 VRRP group. An IPv4 VRRP group can have a maximum of 16 virtual IP addresses.

An IPv4 VRRP group without virtual IP addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

For VRRP to operate correctly in load balancing mode, make sure the virtual IP address of an IPv4 VRRP group is not the IP address of any interfaces in the VRRP group.

Examples

Create IPv4 VRRP group 1 and assign virtual IP address 10.10.10.10 to the VRRP group. Then assign virtual IP address 10.10.10.11 to the VRRP group.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

Related commands

display vrrp

vrrp vrid authentication-mode

Use **vrrp vrid authentication-mode** to configure the authentication mode and the authentication key for an IPv4 VRRP group to send and receive VRRP packets.

Use **undo vrrp vrid authentication-mode** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *string*

undo vrrp vrid *virtual-router-id* **authentication-mode**

Default

Authentication is disabled when a VRRP group sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 8 characters. Its encrypted form is a case-sensitive string of 1 to 41 characters.

Usage guidelines

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication modes:

- **simple**—Simple text authentication.

  The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

- **md5**—MD5 authentication.

  The sender computes a digest for the VRRP packet by using the authentication key and MD5 algorithm, and saves the result to the authentication header. The receiver performs the same operation by using the authentication key and MD5 algorithm, and it compares the result with the content in the authentication header. If the results are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

The MD5 authentication is more secure than the simple text authentication, but it costs more resources.

IMPORTANT:

- You can configure different authentication modes and authentication keys for the VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
- For VRRPv3, this command does not take effect because VRRPv3 does not support authentication.

Examples

Set the authentication mode to **simple** and the authentication key to **Sysname** for VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname
```

Related commands

display vrrp

vrrp version

vrrp vrid follow

Use **vrrp vrid follow** to configure an IPv4 VRRP group to follow a master group.

Use **undo vrrp vrid follow** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **follow** *name*

undo vrrp vrid *virtual-router-id* **follow**

Default

An IPv4 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a subordinate VRRP group to follow a master group. A subordinate VRRP group can forward service traffic.

An IPv4 VRRP group cannot be both a master group and a subordinate group.

An IPv4 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv4 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv4 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 follow abc
```

Related commands

display vrrp binding

vrrp vrid name

vrrp vrid name

Use **vrrp vrid name** to configure an IPv4 VRRP group as a master group and assign a name to it.

Use **undo vrrp vrid name** to remove the configuration.

Syntax

vrrp vrid *virtual-router-id* **name** *name*

undo vrrp vrid *virtual-router-id* **name**

Default

An IPv4 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv4 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv4 VRRP group as a master group by assigning a master group name to it. A VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate VRRP group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different VRRP groups on a device.

Examples

Configure IPv4 VRRP group 1 as a master group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 name abc
```

Related commands

display vrrp binding

vrrp vrid follow

vrrp vrid preempt-mode

Use **vrrp vrid preempt-mode** to enable the preemptive mode for the device in an IPv4 VRRP group and set the preemption delay.

Use **undo vrrp vrid preempt-mode** to disable the preemptive mode for the device in an IPv4 VRRP group.

Use **undo vrrp vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The device operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the device with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

Enable the preemptive mode for the device in VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

Related commands

display vrrp

vrrp vrid priority

Use **vrrp vrid priority** to set the priority of the device in an IPv4 VRRP group.

Use **undo vrrp vrid priority** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

Default

The priority of a device in an IPv4 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each device in a VRRP group by priority. A device with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

Related commands

display vrrp

vrrp vrid track

vrrp vrid shutdown

Use **vrrp vrid shutdown** to disable an IPv4 VRRP group.

Use **undo vrrp vrid shutdown** to enable an IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **shutdown**

undo vrrp vrid *virtual-router-id* **shutdown**

Default

An IPv4 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv4 VRRP group. After this command is configured, the VRRP group stays in **Initialize** state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

Disable IPv4 VRRP group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 shutdown
```

vrrp vrid source-interface

Use **vrrp vrid source-interface** to specify the source interface for an IPv4 VRRP group, instead of the interface where the VRRP group resides, to send and receive VRRP packets.

Use **undo vrrp source-interface** to cancel the specified source interface.

Syntax

vrrp vrid *virtual-router-id* **source-interface** *interface-type interface-number*

undo vrrp vrid *virtual-router-id* **source-interface**

Default

No source interface is specified for a VRRP group. The interface where the VRRP group resides sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

If VRRP group members cannot exchange VRRP packets through the interfaces where the VRRP group resides, use this command to specify interfaces for VRRP packet exchange.

Examples

Specify VLAN-interface 20 as the source interface for VRRP packet exchange in IPv4 VRRP group 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp vrid 10 source-interface vlan-interface 20
```

vrrp vrid timer advertise

Use **vrrp vrid timer advertise** to set the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

Use **undo vrrp vrid timer advertise** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv4 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv4 VRRP group to send VRRP advertisements. The value range for this argument is 10 to 4095 centiseconds. For VRRPv2, the value of the *adver-interval* argument can only be a multiple of 100. For example, if you configure values in the range of 10 to 100, 101 to 200, and 4001 to 4095, the actual values are 100, 200, and 4100, respectively. For VRRPv3, the configured value for the *adver-interval* argument takes effect.

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

In VRRPv2, all routers in an IPv4 VRRP group must have the same interval for sending VRRP advertisements.

In VRRPv3, the routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × recorded interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to set a larger interval.

Examples

Configure the master in IPv4 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

Related commands

display vrrp

vrrp vrid track

Use **vrrp vrid track** to associate a VRRP group or the VFs in a VRRP group with a track entry.

Use **undo vrrp vrid track** to remove the association between a VRRP group or the VFs in a VRRP group and a track entry.

Syntax

vrrp vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

undo vrrp vrid *virtual-router-id* **track** [*track-entry-number*] [**forwarder-switchover** | **priority reduced** | **switchover** | **weight reduced**]

Default

A VRRP group and the VFs in a VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip *ip-address*: Enables the LVF on the router to take over the role of the AVF at the specified IP address immediately after the specified track entry changes to the Negative state. The *ip-address* argument specifies the IP address of a member router. You can use the **display vrrp verbose** command to view the IP addresses of the members.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [*weight-reduced*]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *weight-reduced* argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The weight of VFs decreases by a specified value.
- The router immediately takes over as the master if it is a backup.
- The LVF on the router immediately takes over the role of the AVF at the specified IP address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority or VF weight.
- The failed master router becomes the master again.
- The failed AVF becomes active again.

Before executing this command, create a VRRP group on the interface and assign a virtual IP address to the VRRP group.

You can create a track entry by using the **track** command before or after you associate it with a VRRP group or the VFs in a VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp vrid track** command removes all associations between track entries and the VRRP group or VFs in the VRRP group.

The **vrrp vrid track priority reduced** command and the **vrrp vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv4 VRRP group is operating in load balancing mode:

- The **forwarder-switchover member-ip** *ip-address* option.
- The **weight reduced** *weight-reduced* option.
- The **weight reduced** keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover occurs when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
```

Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IP address of 10.1.1.3 immediately when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 forwarder-switchover member-ip 10.1.1.3
```

Associate the VFs of IPv4 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> sysname-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 50
```

Related commands

display vrrp

vrrp vrid vrrpv3-send-packet

Use **vrrp vrid vrrpv3-send-packet** to set the packet sending mode for IPv4 VRRPv3.

Use **undo vrrp vrid vrrpv3-send-packet** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **vrrpv3-send-packet** { **v2-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **vrrpv3-send-packet**

Default

A router configured with IPv4 VRRPv3 sends only VRRPv3 packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

v2-only: Sends VRRPv2 packets only.

v2v3-both: Sends both VRRPv2 and VRRPv3 packets.

Usage guidelines

This command takes effect only on IPv4 VRRPv3.

The packet sending mode for IPv4 VRRPv3 takes effect only on outgoing VRRP packets. A router configured with VRRPv3 can process incoming VRRPv2 and VRRPv3 packets.

If you set the packet sending mode for IPv4 VRRPv3 and configure VRRP packet authentication, authentication information will be carried in outgoing VRRPv2 packets but not in outgoing VRRPv3 packets.

The VRRP advertisement interval is set in centiseconds by using the **vrrp vrid timer advertise** command. The VRRP advertisement interval carried in VRRPv2 packets sent from routers configured with VRRPv3 might be different from the configured value. For information about the VRRP advertisement interval, see the **vrrp vrid timer advertise** command.

Examples

Configure VRRP group 1 to send both VRRPv2 and VRRPv3 packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 version-3 send-packet-mode v2v3-both
```

Related commands

display vrrp

IPv6 VRRP commands

VRRP does not take effect on member ports of aggregation groups.

display vrrp ipv6

Use **display vrrp ipv6** to display the states of IPv6 VRRP groups.

Syntax

display vrrp ipv6 [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv6 VRRP group information. If you do not specify the **verbose** keyword, the command displays brief IPv6 VRRP group information.

Usage guidelines

If no interface or VRRP group is specified, this command displays the states of all IPv6 VRRP groups.

If only an interface is specified, this command displays the states of all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays the states of the specified IPv6 VRRP group on the specified interface.

Examples

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 1
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type       IP
 ------------------------------------------------------------------------
 Vlan2              1     Master       150     100     None     FE80::1
```

Table 8 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
ND sending interval	Sending interval for ND packets. This field is displayed only after you configure the **vrrp ipv6 send-nd** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Adver Timer	VRRP advertisement sending interval in centiseconds.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 ND sending interval : 120 sec
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Master
     Config Pri       : 150               Running Pri  : 150
     Preempt Mode     : Yes               Delay Time   : 10
     Auth Type        : None
```

```
  Virtual IP       : FE80::1
  Virtual MAC      : 0000-5e00-0201
  Master IP        : FE80::2
  Config Role      : Master
  Name             : abc
VRRP Track Information:
  Track Object   : 1                    State : Positive   Pri Reduced : 50

Interface Vlan-interface2
  VRID             : 2                    Adver Timer  : 100
  Admin Status     : Up                   State        : Backup
  Config Pri       : 80                   Running Pri  : 80
  Preempt Mode     : Yes                  Delay Time   : 0
  Become Master    : 2450ms left
  Auth Type        : None
  Virtual IP       : FE80::11
  Virtual MAC      : 0000-5e00-0202
  Master IP        : FE80::12

Interface Vlan-interface2
  VRID             : 3                    Adver Timer  : 100
  Admin Status     : Up                   State        : Master
  Config Pri       : 100                  Running Pri  : 100
  Preempt Mode     : Yes                  Delay Time   : 0
  Auth Type        : None
  Virtual IP       : FE80::10
  Virtual MAC      : 0000-5e00-0203
  Master IP        : FE80::2
  Config Role      : Subordinate
  Follow Name      : abc
```

Table 9 Command output (in standard mode)

Field	Description
Running Mode	VRRP operating mode (standard mode).
ND sending interval	Sending interval for ND packets. This field is displayed only after you configure the **vrrp ipv6 send-nd** command.
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.

Field	Description
Config Pri	Configured priority of the router, which is configured by using the **vrrp ipv6 vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address of the VRRP group.
Virtual MAC	Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master.
Master IP	Link-local address of the interface where the master resides.
Config Role	The configured role of the IPv6 VRRP group to which the router belongs. • **Master**. • **Subordinate**.
Name	Master group name assigned to the IPv6 VRRP group. This field is displayed only after you configure the **vrrp ipv6 vrid name** command.
Follow Name	Name of the master VRRP group that the IPv6 VRRP group follows. This field is displayed only after you configure the **vrrp ipv6 vrid follow** command.
VRRP Track Information	Track entry information. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry which is associated with the VRRP group.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the state of the associated track entry becomes Negative.
Switchover	Switchover mode. When the state of the associated track entry becomes Negative, the backup immediately becomes the master.

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 1
 Interface          VRID  State        Running Address            Active
```

```
                                      Pri
------------------------------------------------------------------------
Vlan2               1     Master      150     FE80::1             Local
-----               VF 1  Active      255     000f-e2ff-4011      Local
```

Table 10 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number) or VF ID.
State	• For a VRRP group, this field indicates the state of the router in the VRRP group. The state can be **Master**, **Backup**, **Initialize**, or **Inactive**. • For a VF, this field indicates the state of the VF in the VRRP group. The state can be **Active**, **Listening**, or **Initialize**.
Running Pri	• For a VRRP group, this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. • For a VF, this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the state of the track entry changes.
Address	• For a VRRP group, this field indicates the virtual IP address of the VRRP group. • For a VF, this field indicates the virtual MAC address of the VF.
Active	• For a VRRP group, this field indicates the link-local address of the interface where the master resides. If the current router is the master, this field displays **local**. • For a VF, this field indicates the link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Load Balance
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 150                Running Pri  : 150
     Preempt Mode   : Yes                Delay Time   : 5
     Auth Type      : None
     Virtual IP     : FE80::10
     Member IP List : FE80::3 (Local, Master)
                      FE80::2 (Backup)
     Master IP      : FE80::3
   VRRP Track Information:
```

```
  Track Object   : 1                    State : Positive   Pri Reduced : 50
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-4011 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-4012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : FE80::2
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
Interface Vlan-interface2
  VRID           : 11                   Adver Timer  : 100
  Admin Status   : Up                   State        : Backup
  Config Pri     : 80                   Running Pri  : 80
  Preempt Mode   : Yes                  Delay Time   : 0
  Become Master  : 2450ms left
  Auth Type      : None
  Virtual IP     : FE80::11
  Member IP List : FE80::3 (Local, Backup)
                   FE80::2 (Master)
  Master IP      : FE80::2
Forwarder Information: 2 Forwarders 1 Active
  Config Weight  : 255
  Running Weight : 255
 Forwarder 01
  State          : Active
  Virtual MAC    : 000f-e2ff-40b1 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 127
  Active         : FE80::2
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-40b2 (Owner)
  Owner ID       : 0000-5e01-1101
  Priority       : 255
  Active         : local
```

Table 11 Command output (in load balancing mode)

Field	Description
Running Mode	VRRP operating mode (load balancing mode).

Field	Description
Total number of virtual routers	Total number of VRRP groups.
Interface	Interface where the VRRP group is configured.
VRID	Virtual router ID (VRRP group number).
Adver Timer	VRRP advertisement sending interval in centiseconds.
Admin Status	Administrative status: **Up** or **Down**.
State	Status of the router in the VRRP group: • **Master**. • **Backup**. • **Initialize**. • **Inactive**.
Config Pri	Configured priority of the router, which is configured by using the **vrrp ipv6 vrid priority** command.
Running Pri	Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes.
Preempt Mode	Preemptive mode: • **Yes**. • **No**.
Delay Time	Preemption delay in centiseconds.
Become Master	Time (in milliseconds) that a backup router has to wait before it becomes the master. This field is displayed only when the router is a backup.
Auth Type	Authentication type. Only **none** is available, which means no authentication is required.
Virtual IP	Virtual IP address list of the VRRP group.
Member IP List	IP addresses of the member devices in the VRRP group: • **Local**—IP address of the local router. • **Master**—IP address of the master. • **Backup**—IP address of the backup.
VRRP Track Information	Track entry that is associated with the VRRP group. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry to be monitored. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Pri Reduced	Value by which the priority decreases when the status of the associated track entry becomes Negative. This field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Switchover	Switchover mode. When the status of the associated track entry becomes Negative, the backup immediately becomes the master.
Forwarder Information: 2 Forwarders 1 Active	VF information: Two VFs exist and one is the AVF.

Field	Description
Config Weight	Configured weight of the VF: 255.
Running Weight	Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes.
Forwarder 01	Information about VF 01.
State	VF state: • **Active**. • **Listening**. • **Initialize**.
Virtual MAC	Virtual MAC address of the VF.
Owner ID	Real MAC address of the VF owner.
Priority	VF priority in the range of 1 to 255.
Active	Link-local address of the interface where the AVF resides. If the current VF is the AVF, this field displays **local**.
Forwarder Weight Track Configuration	VF weight Track configuration. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Track Object	Track entry which is associated with the VFs. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
State	Track entry state: • **Negative**. • **Positive**. • **NotReady**.
Weight Reduced	Value by which the weights of the VFs decrease when the state of the associated track entry changes to Negative. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Forwarder Switchover Track Information:	VF switchover Track configuration. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.
Member IP	IPv6 address of a member device. The field is displayed only after you configure the **vrrp ipv6 vrid track** command.

display vrrp ipv6 binding

Use **display vrrp ipv6 binding** to display master-to-subordinate IPv6 VRRP group bindings.

Syntax

display vrrp ipv6 binding [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **name** *name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The interface must be an interface to which master IPv6 VRRP groups belong.

vrid *virtual-router-id*: Specifies a master IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name *name*: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

If you do not specify any parameters, this command displays all master-to-subordinate IPv6 VRRP group bindings.

If you specify an interface but do not specify the virtual router ID of a master IPv6 VRRP group, this command displays all master-to-subordinate IPv6 VRRP group bindings on the specified interface.

If you specify an interface and the virtual router ID of a master IPv6 VRRP group, this command displays the binding information about the specified master VRRP group on the specified interface.

Examples

Display master-to-subordinate IPv6 VRRP group bindings.

```
<Sysname> display vrrp ipv6 binding
IPv6 virtual router binding information:
  Total number of master virtual routers            : 1
  Total number of subordinate virtual routers       : 2
  Interface : Vlan2                    Master VRID : 1
  Name      : a                        Status      : Backup
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 4

  Interface : --                       Master VRID : --
  Name      : c                        Status      : --
  Subordinate virtual routers : 1
    Interface : Vlan2                  VRID        : 5
```

Table 12 Command output

Field	Description
Total number of master virtual routers	Total number of master IPv6 VRRP groups.
Total number of subordinate virtual routers	Total number of subordinate IPv6 VRRP groups.
Interface	Interface to which the master IPv6 VRRP group belongs. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Master VRID	Virtual router ID of the master IPv6 VRRP group. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Name	Name of the master IPv6 VRRP group.
Status	Status of the router in the master IPv6 VRRP group:

Field	Description
	• **Master**. • **Backup**. • **Initialize**. • **Inactive**. If the master IPv6 VRRP group does not exist, this field displays two hyphens (**--**).
Subordinate virtual routers	Number of subordinate IPv6 VRRP groups.
Interface	Interface to which the subordinate IPv6 VRRP group belongs.
VRID	Virtual router ID of the subordinate IPv6 VRRP group.

Related commands

vrrp ipv6 vrid follow

vrrp ipv6 vrid name

display vrrp ipv6 statistics

Use **display vrrp ipv6 statistics** to display statistics for IPv6 VRRP groups.

Syntax

display vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command displays statistics for all IPv6 VRRP groups.

If only an interface is specified, this command displays statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command displays statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Display statistics for all IPv6 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 statistics
 Interface              : Vlan-interface2
 VRID                   : 1
 CheckSum Errors        : 0          Version Errors               : 0
```

```
 Invalid Pkts Rcvd       : 0          Unexpected Pkts Rcvd          : 0
 Hop Limit Errors        : 0          Advertisement Interval Errors : 0
 Invalid Auth Type       : 0          Auth Failures                 : 0
 Packet Length Errors    : 0          Auth Type Mismatch            : 0
 Become Master           : 1          Address List Errors           : 0
 Adver Rcvd              : 0          Priority Zero Pkts Rcvd       : 0
 Adver Sent              : 425        Priority Zero Pkts Sent       : 0
IP Owner Conflicts      : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Display statistics for all IPv6 VRRP groups when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 statistics
 Interface               : Vlan-interface2
 VRID                    : 1
 CheckSum Errors         : 0          Version Errors                : 0
 Invalid Pkts Rcvd       : 0          Unexpected Pkts Rcvd          : 0
 Hop Limit Errors        : 0          Advertisement Interval Errors : 0
 Invalid Auth Type       : 0          Auth Failures                 : 0
 Packet Length Errors    : 0          Auth Type Mismatch            : 0
 Become Master           : 39         Address List Errors           : 0
 Become AVF              : 13         Packet Option Errors          : 0
 Adver Rcvd              : 2562       Priority Zero Pkts Rcvd       : 1
 Adver Sent              : 16373      Priority Zero Pkts Sent       : 49
 Request Rcvd            : 2          Reply Rcvd                    : 10
 Request Sent            : 12         Reply Sent                    : 2
 Release Rcvd            : 0          VF Priority Zero Pkts Rcvd    : 1
 Release Sent            : 0          VF Priority Zero Pkts Sent    : 11
 Redirect Timer Expires  : 1          Time-out Timer Expires        : 0

 Global statistics
 CheckSum Errors         : 0
 Version Errors          : 0
 VRID Errors             : 0
```

Table 13 Command output (in standard mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.

Field	Description
Hop Limit Errors	Number of packets with hop limit errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.
Become Master	Number of times that the router has been elected as the master.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
Adver Rcvd	Number of received advertisements.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
Adver Sent	Number of sent advertisements.
IP Owner Conflicts	Number of VRRP packets that the local router (IP address owner) has received from conflicting IP address owners.
Global statistics	Global statistics for all IPv6 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Table 14 Command output (in load balancing mode)

Field	Description
Interface	Interface where the VRRP group is configured.
VRID	VRRP group number.
CheckSum Errors	Number of packets with checksum errors.
Version Errors	Number of packets with version errors.
Invalid Pkts Rcvd	Number of received packets of invalid packet types.
Unexpected Pkts Rcvd	Number of received unexpected packets.
Advertisement Interval Errors	Number of packets with advertisement interval errors.
Hop Limit Errors	Number of packets with hop limit errors.
Auth Failures	Number of packets with authentication failures.
Invalid Auth Type	Number of packets with authentication failures because of invalid authentication types.
Auth Type Mismatch	Number of packets with authentication failures because of mismatching authentication types.
Packet Length Errors	Number of packets with VRRP packet length errors.
Address List Errors	Number of packets with virtual IP address list errors.

Field	Description
Become Master	Number of times that the router has been elected as the master.
Redirect Timer Expires	Number of times that the redirect timer expired.
Become AVF	Number of times that the VF has been elected as the AVF.
Time-out Timer Expires	Number of times that the time-out timer expired.
Adver Rcvd	Number of received advertisements.
Request Rcvd	Number of received requests.
Adver Sent	Number of sent advertisements.
Request Sent	Number of sent requests.
Reply Rcvd	Number of received replies.
Release Rcvd	Number of received release packets.
Reply Sent	Number of sent replies.
Release Sent	Number of sent release packets.
Priority Zero Pkts Rcvd	Number of received advertisements with the router priority of 0.
VF Priority Zero Pkts Rcvd	Number of received advertisements with the VF priority of 0.
Priority Zero Pkts Sent	Number of sent advertisements with the router priority of 0.
VF Priority Zero Pkts Sent	Number of sent advertisements with the VF priority of 0.
Packet Option Errors	Number of packet option errors.
Global statistics	Global statistics for all IPv6 VRRP groups.
CheckSum Errors	Total number of packets with checksum errors.
Version Errors	Total number of packets with version errors.
VRID Errors	Total number of packets with VRID errors.

Related commands

reset vrrp ipv6 statistics

reset vrrp ipv6 statistics

Use **reset vrrp ipv6 statistics** to clear statistics for IPv6 VRRP groups.

Syntax

reset vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

If no interface or VRRP group is specified, this command clears statistics for all IPv6 VRRP groups.

If only an interface is specified, this command clears statistics for all IPv6 VRRP groups on the specified interface.

If both an interface and an IPv6 VRRP group are specified, this command clears statistics for the specified IPv6 VRRP group on the specified interface.

Examples

Clear statistics for all IPv6 VRRP groups on all interfaces.

```
<Sysname> reset vrrp ipv6 statistics
```

Related commands

display vrrp ipv6 statistics

vrrp ipv6 dscp

Use **vrrp ipv6 dscp** to set a DSCP value for IPv6 VRRP packets.

Use **undo vrrp ipv6 dscp** to restore the default.

Syntax

vrrp ipv6 dscp *dscp-value*

undo vrrp ipv6 dscp

Default

The DSCP value for IPv6 VRRP packets is 56.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for IPv6 VRRP packets, in the range of 0 to 63.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

Set the DSCP value to 30 for IPv6 VRRP packets.

```
<Sysname> system-view
[Sysname] vrrp ipv6 dscp 30
```

vrrp ipv6 mode

Use **vrrp ipv6 mode** to specify the operating mode for IPv6 VRRP.

Use **undo vrrp ipv6 mode** to restore the default.

Syntax

vrrp ipv6 mode load-balance

undo vrrp ipv6 mode

Default

IPv6 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

Usage guidelines

For IPv6 VRRP to operate correctly in load balancing mode, make sure the virtual IPv6 address of an IPv6 VRRP group is not the IPv6 address of any interfaces in the VRRP group.

After you create IPv6 VRRP groups on the router, you can use this command to modify their operating mode. All IPv6 VRRP groups on the router operate in the specified mode.

Examples

Specify the load balancing mode for IPv6 VRRP.

```
<Sysname> system-view
[Sysname] vrrp ipv6 mode load-balance
```

Related commands

display vrrp ipv6

vrrp ipv6 send-nd

Use **vrrp ipv6 send-nd** to enable periodic sending of ND packets for IPv6 VRRP.

Use **undo vrrp ipv6 send-nd** to disable periodic sending of ND packets for IPv6 VRRP.

Syntax

vrrp ipv6 send-nd [**interval** *interval*]

undo vrrp ipv6 send-nd

Default

Periodic sending of ND packets is disabled for IPv6 VRRP.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sending interval in the range of 30 to 1200 seconds. The default value is 120 seconds.

Usage guidelines

This command ensures that the MAC address entry for the virtual MAC address of an IPv6 VRRP group can be updated on downstream devices in a timely manner.

This command takes effect only in VRRP standard mode.

If you change the sending interval for ND packets, the configuration takes effect at the next sending interval.

The master sends the first ND packet at a random time in the second half of the set interval after you execute the **vrrp ipv6 send-nd** command. This prevents too many ND packets from being sent at the same time.

The sending interval for ND packets might be much longer than the set interval when the following conditions are met:

- Multiple IPv6 VRRP groups exist on the device.
- A short sending interval is set.

Examples

Enable periodic sending of ND packets for IPv6 VRRP and set the sending interval to 200 seconds.

```
<Sysname> system-view
[Sysname] vrrp ipv6 send-nd interval 200
```

vrrp ipv6 vrid

Use **vrrp ipv6 vrid** to create an IPv6 VRRP group and assign a virtual IPv6 address to it, or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use **undo vrrp ipv6 vrid** to remove all configurations of an IPv6 VRRP group, or to remove a virtual IPv6 address from an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** [*virtual-address* [**link-local**]]]

Default

No IPv6 VRRP groups exist.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IPv6 address. If you do not specify this option, the **undo vrrp ipv6 vrid** command removes all virtual IPv6 addresses from the specified IPv6 VRRP group.

link-local: Specifies a link-local address as the virtual IPv6 address.

Usage guidelines

You can execute this command multiple times to assign multiple virtual IPv6 addresses to an IPv6 VRRP group. An IPv6 VRRP group can have a maximum of 16 virtual IPv6 addresses.

The first virtual IPv6 address that you assign to an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address.

An IPv6 VRRP group without virtual IPv6 addresses configured can exist on a device provided that other settings (for example, priority and preemption mode) are available. Such a VRRP group stays in inactive state and does not function.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

Create IPv6 VRRP group 1 and assign virtual IPv6 address fe80::10 to the VRRP group. Then assign virtual IPv6 address 1::10 to the VRRP group.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid follow

Use **vrrp ipv6 vrid follow** to configure an IPv6 VRRP group to follow a master group.

Use **undo vrrp ipv6 vrid follow** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **follow** *name*

undo vrrp ipv6 vrid *virtual-router-id* **follow**

Default

An IPv6 VRRP group does not follow a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group by its name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a subordinate VRRP group to follow a master group. A subordinate IPv6 VRRP group can forward service traffic.

An IPv6 VRRP group cannot be both a master group and a subordinate group.

An IPv6 VRRP group stays in **Inactive** state if it is configured to follow a nonexistent master VRRP group.

If an IPv6 VRRP group in **Inactive** or **Initialize** state follows a master group that is not in **Inactive** state, the state of the VRRP group does not change.

Examples

Configure IPv6 VRRP group 1 to follow master group **abc**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 follow abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid name

vrrp ipv6 vrid name

Use **vrrp ipv6 vrid name** to configure an IPv6 VRRP group as a master group and assign a name to it.

Use **undo vrrp ipv6 vrid name** to remove the configuration.

Syntax

vrrp ipv6 vrid *virtual-router-id* **name** *name*

undo vrrp ipv6 vrid *virtual-router-id* **name**

Default

An IPv6 VRRP group does not act as a master group.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

name: Specifies a master IPv6 VRRP group name, a case-sensitive string of 1 to 20 characters.

Usage guidelines

This command configures an IPv6 VRRP group as a master group through assigning a master group name to it. An IPv6 VRRP group that follows the master group is a subordinate VRRP group. The master VRRP group exchanges VRRP packets among member devices. The subordinate group does not exchange VRRP packets and follows the state of the master group. Both the master and subordinate VRRP groups can forward service traffic.

You cannot assign the same master VRRP group name to different IPv6 VRRP groups on a device.

Examples

Configure IPv6 VRRP group 1 as a master VRRP group and assign master group name **abc** to it.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 name abc
```

Related commands

display vrrp ipv6 binding

vrrp ipv6 vrid follow

vrrp ipv6 vrid preempt-mode

Use **vrrp ipv6 vrid preempt-mode** to enable the preemptive mode for the router in an IPv6 VRRP group and set the preemption delay.

Use **undo vrrp ipv6 vrid preempt-mode** to disable the preemptive mode for the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The router operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies the preemption delay in the range of 0 to 180000 in centiseconds.

Usage guidelines

In non-preemptive mode, the master router acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup sends VRRP advertisements when it detects that it has a higher priority than the master. Then the backup takes over as the master and the previous master becomes a backup. This mechanism ensures that the master is always the router with the highest priority.

You can configure the VRRP preemption delay for the following purposes:

- Avoid frequent state changes among members in a VRRP group.
- Provide the backups with enough time to collect information (such as routing information).

A backup does not immediately become the master after it receives an advertisement with a lower priority than the local priority. Instead, it waits for a period of time before taking over.

Examples

Enable the preemptive mode for VRRP group 1, and set the preemption delay to 5000 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 5000
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid priority

Use **vrrp ipv6 vrid priority** to set the priority of the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid priority** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

Default

The priority of a router in an IPv6 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher value indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Set the priority of the switch to 150 in VRRP group 1 on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid shutdown

Use **vrrp ipv6 vrid shutdown** to disable an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid shutdown** to enable an IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **shutdown**

undo vrrp ipv6 vrid *virtual-router-id* **shutdown**

Default

An IPv6 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv6 VRRP group. After this command is configured, the VRRP group stays in **Initialize** state, and its configurations remain unchanged. You can change the configuration of the VRRP group, and your changes take effect when you enable the VRRP group again.

Examples

Disable IPv6 VRRP group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 shutdown
```

vrrp ipv6 vrid timer advertise

Use **vrrp ipv6 vrid timer advertise** to set the interval at which the master in an IPv6 VRRP group sends VRRP advertisements.

Use **undo vrrp ipv6 vrid timer advertise** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv6 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv6 VRRP group to send VRRP advertisements, in the range of 100 to 4095 centiseconds.

Usage guidelines

The master in an IPv6 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to set the interval at which the master sends VRRP advertisements.

As a best practice to maintain system stability, set the VRRP advertisement interval to be greater than 100 centiseconds.

The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive any VRRP advertisement when the timer (3 × VRRP advertisement sending interval + Skew_Time) expires, it regards the master as failed and takes over.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified timer and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

Configure the master in IPv6 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid track

Use **vrrp ipv6 vrid track** to associate an IPv6 VRRP group or the VFs in an IPv6 VRRP group with a track entry.

Use **undo vrrp ipv6 vrid track** to remove the association between an IPv6 VRRP group or the VFs in an IPv6 VRRP group and a track entry.

Syntax

vrrp ipv6 vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ipv6-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

undo vrrp ipv6 vrid *virtual-router-id* **track** [*track-entry-number*] [**forwarder-switchover** | **priority reduced** | **switchover** | **weight reduced**]]

Default

An IPv6 VRRP group and the VFs in an IPv6 VRRP group are not associated with any track entries.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry by its number in the range of 1 to 1024.

forwarder-switchover member-ip *ipv6-address*: Enables the LVF on the router to take over the role of the AVF at the specified IPv6 address immediately after the specified track entry changes to the Negative state. The *ipv6-address* argument specifies the IPv6 address of a member router. You can use the **display vrrp ipv6 verbose** command to view the IPv6 addresses of the members.

priority reduced [*priority-reduced*]: Reduces the priority of the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *priority-reduced* argument is 1 to 255, and the default value is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the Negative state.

weight reduced [*weight-reduced*]: Reduces the weight of all VFs on the router in the VRRP group by the specified value when the state of the specified track entry changes to Negative. The value range for the *weight-reduced* argument is 1 to 255, and the default value is 30.

Usage guidelines

When the associated track entry changes to the Negative state, one of the following events occurs depending on your configuration:

- The priority of the router in the VRRP group decreases by a specified value.
- The weight of VFs decreases by a specified value.
- The router immediately takes over as the master if it is a backup.
- The LVF on the router immediately takes over the role of the AVF at the specified IPv6 address.

When the track entry changes from Negative to Positive or NotReady, one of the following events occurs:

- The router automatically restores its priority or VF weight.
- The failed master router becomes the master again.
- The failed AVF becomes active again.

Before executing this command, create an IPv6 VRRP group on the interface and assign a virtual IPv6 address to the IPv6 VRRP group.

You can create a track entry by using the **track** command before or after you associate it with an IPv6 VRRP group or the VFs in an IPv6 VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

If no track entry is specified, the **undo vrrp ipv6 vrid track** command removes all associations between track entries and the IPv6 VRRP group or VFs in the IPv6 VRRP group.

The **vrrp ipv6 vrid track priority reduced** command and the **vrrp ipv6 vrid track switchover** command do not take effect on an IP address owner. If you configure the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.

The following parameters take effect only when the IPv6 VRRP group is operating in load balancing mode:

- The **forwarder-switchover member-ip** *ip-address* option.
- The **weight reduced** *weight-reduced* option.
- The **weight reduced** keyword.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255. The priority does not change with the weight. When the upstream link of the VF owner fails, an LVF must take over as the AVF. The switchover happens when the weight of the VF owner drops below the lower limit of failure. This requires that the reduced weight for the VF owner be higher than 245.

Examples

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the router priority by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 priority reduced 50
```

Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Enable the LVF to take over the role of the AVF at the IPv6 address of 1::3 immediately when the state of track entry 1 changes to Negative.)

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 forwarder-switchover member-ip 1::3
```

Associate the VFs of IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1. Decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to Negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track 1 weight reduced 50
```

Related commands

display vrrp ipv6

Release 3208

This release has the following changes:

- New feature: MAC address information display for 802.1X users in 802.1X VLANs of a specific type
- New feature: Authorization CAR action for an ISP domain
- New feature: 802.1X client
- New feature: MAC address information display for MAC authentication users in MAC authentication VLANs of a specific type
- Modified feature: Configuring the hash seed for global link aggregation load sharing
- Modified feature: Specifying a RADIUS or HWTACACS server

New feature: MAC address information display for 802.1X users in 802.1X VLANs of a specific type

Displaying MAC address information of 802.1X users in 802.1X VLANs of a specific type

Execute **display** commands in any view.

Task	Command
Display MAC address information of 802.1X users in 802.1X VLANs of a specific type.	**display dot1x mac-address** { **auth-fail-vlan** | **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Command reference

display dot1x mac-address

Use **display dot1x mac-address** to display MAC address information of 802.1X users in 802.1X VLANs of a specific type.

Syntax

display dot1x mac-address { **auth-fail-vlan** \| **critical-vlan** \| **guest-vlan** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

auth-fail-vlan: Specifies the 802.1X Auth-Fail VLAN.

critical-vlan: Specifies the 802.1X critical VLAN.

guest-vlan: Specifies the 802.1X guest VLAN.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MAC address information of 802.1X users in the specified 802.1X VLAN on all ports.

Usage guidelines

This command displays rough statistics. It might not fully display the specified information when a large number of 802.1X users perform authentication frequently.

Examples

Display MAC address information of 802.1X users in the 802.1X Auth-Fail VLAN on all ports.

```
<Sysname> display dot1x mac-address auth-fail-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1        Auth-Fail VLAN: 3    Aging time: N/A
MAC addresses: 8
  0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
  0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2        Auth-Fail VLAN: 5    Aging time: 30 sec
MAC addresses: 2
  0801-2700-9427    0801-2700-2341
```

Table 1 Command output

Field	Description
Total MAC addresses	Total number of MAC addresses in the specified VLAN on the specified port or all ports.
Interface	Access port of 802.1X users.
Type VLAN	VLAN information for 802.1X users. The *Type* argument has the following values: • Auth-Fail VLAN. • Critical VLAN. • Guest VLAN.
Aging time	MAC address aging time in seconds. This field displays **N/A** if the MAC addresses do not age out.
MAC addresses	Number of matching MAC addresses on a port.
xxxx-xxxx-xxxx	MAC address.

Related commands

dot1x auth-fail vlan

dot1x critical vlan

dot1x guest-vlan

New feature: Authorization CAR action for an ISP domain

Configuring an authorization CAR action for an ISP domain

The CAR action attribute controls the traffic flows of authenticated users.

If the server does not authorize a CAR action to an authenticated user, the device assigns the domain's authorization CAR action to the user.

For portal users, you can configure an authorization CAR action in their preauthentication domain to control their traffic flows before they pass authentication.

To configure an authorization CAR action for an ISP domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter ISP domain view.	**domain** *isp-name*	N/A
3. Configure an authorization CAR action for the ISP domain.	**authorization-attribute car inbound cir** *committed-information-rate* [**pir** *peak-information-rate*] **outbound cir** *committed-information-rate* [**pir** *peak-information-rate*]	By default, no authorization CAR action is configured for an ISP domain.

Command reference

authorization-attribute car

Use **authorization-attribute car** to configure an authorization CAR action for an ISP domain.

Use **undo authorization-attribute car** to restore the default.

Syntax

authorization-attribute car inbound cir *committed-information-rate* [**pir** *peak-information-rate*] **outbound cir** *committed-information-rate* [**pir** *peak-information-rate*]

undo authorization-attribute car

Default

No authorization CAR action is configured for an ISP domain.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

inbound: Specifies the upload rate of users.

outbound: Specifies the download rate of users.

cir *committed-information-rate*: Specifies the committed information rate in kbps, in the range of 1 to 4194303.

pir *peak-information-rate*: Specifies the peak information rate in kbps, in the range of 1 to 4194303. If you do not specify this option, the CAR action does not restrict users by peak information rate.

Usage guidelines

If the server does not authorize a CAR action to an authenticated user, the device assigns the domain's authorization CAR action to the user.

For portal users, you can configure an authorization CAR action in their preauthentication domain to control their traffic flows before they pass authentication.

Examples

Configure an authorization CAR action for ISP domain **test**. In the CAR action attribute, the CIR for upload rate of users is 1111 kbps, and the CIR for download rate of users is 2222 kbps.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute car inbound cir 1111 outbound cir 2222
```

Related commands

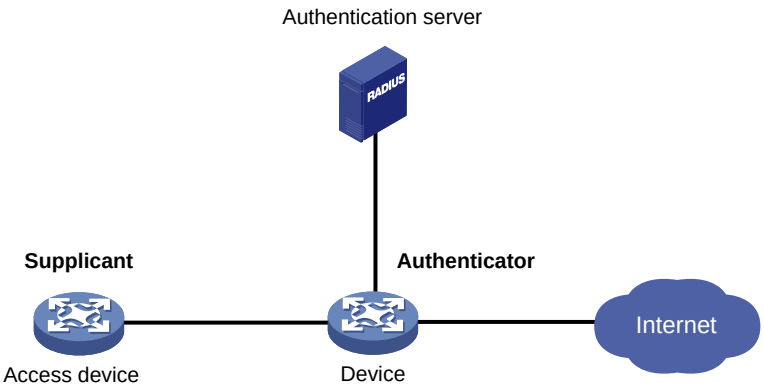
display domain

New feature: 802.1X client

Configuring 802.1X client

As shown in Figure 1, the 802.1X client feature allows the access device to act as the supplicant in the 802.1X architecture. For information about the 802.1X architecture, see "802.1X overview."

Figure 1 802.1X client network diagram



802.1X client configuration task list

Tasks at a glance
(Required.) Enabling the 802.1X client feature
(Required.) Configuring an 802.1X client username and password
(Optional.) Configuring an 802.1X client MAC address
(Required.) Specifying an 802.1X client EAP authentication method
(Optional.) Configuring an 802.1X client anonymous identifier
(Optional.) Specifying an SSL client policy

Enabling the 802.1X client feature

Before enabling the 802.1X client feature, make sure you have configured 802.1X authentication on the authenticator. For information about 802.1X configuration, see "Configuring 802.1X."

To enable the 802.1X client feature on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the 802.1X client feature.	**dot1x supplicant enable**	By default, the 802.1X client feature is disabled.

Configuring an 802.1X client username and password

An 802.1X client-enabled device uses the configured username and password for 802.1X authentication.

Make sure the username and password configured on the device is consistent with the username and password configured on the authentication server. If any inconsistency occurs, the device cannot pass 802.1X authentication to access the network.

To configure an 802.1X client username and password on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an 802.1X client username.	**dot1x supplicant username** *username*	By default, no 802.1X client username exists.
4. Set an 802.1X client password.	**dot1x supplicant password** { **cipher** | **simple** } *string*	By default, no 802.1X client password exists.

Configuring an 802.1X client MAC address

The authenticator adds the MAC address of an authenticated 802.1X client to the MAC address table and then assigns access rights to the client.

You can use either of the following methods to configure a unique MAC address for each interface:

- Execute the **mac-address** command in Ethernet interface view. For information about this command, see *Layer 2—LAN Switching Command Reference*.
- Configure an 802.1X client MAC address.

To configure an 802.1X client MAC address on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Configure an 802.1X client MAC address.	**dot1x supplicant mac-address** *mac-address*	By default, an Ethernet interface uses the interface's MAC address for 802.1X client authentication. If the interface's MAC address is unavailable, the interface uses the device's MAC address for 802.1X client authentication.

Specifying an 802.1X client EAP authentication method

An 802.1X client-enabled device supports the following EAP authentication methods:

- MD5-Challenge.
- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

An 802.1X authenticator supports both the EAP relay and EAP termination modes. Support of the EAP authentication methods for the two modes varies.

- The MD5-Challenge EAP authentication supports both modes.
- Other EAP authentication methods support only the EAP relay mode.

For information about EAP relay and EAP termination, see "Configuring 802.1X."

To specify an 802.1X client EAP authentication method on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an 802.1X client EAP authentication method.	**dot1x supplicant eap-method** { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }	By default, an 802.1X client-enabled interface uses the MD5-Challenge EAP authentication. Make sure the specified 802.1X client EAP authentication method is supported by the authentication server.

Configuring an 802.1X client anonymous identifier

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username at the first authentication phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

- PEAP-MSCHAPv2.

- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

To configure an 802.1X client anonymous identifier on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an 802.1X client anonymous identifier.	**dot1x supplicant anonymous identify** *identifier*	By default, no 802.1X client anonymous identifier exists.

Specifying an SSL client policy

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X client authentication process is as follows:

- **The first phase**—The device acts as an SSL client to negotiate with the SSL server.

  The SSL client uses the SSL parameters defined in the specified SSL client policy to establish a connection with the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policy configuration, see "Configuring SSL."
- **The second phase**—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

To specify an SSL client policy on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an SSL client policy.	**dot1x supplicant ssl-client-policy** *policy-name*	By default, an 802.1X client-enabled interface uses the default SSL client policy.

Displaying and maintaining 802.1X client

Execute **display** commands in any view.

Task	Command
Display 802.1X client information.	**display dot1x supplicant** [**interface** *interface-type interface-number*]

802.1X client commands

display dot1x supplicant

Use **display dot1x supplicant** to display 802.1X client authentication information.

Syntax

display dot1x supplicant [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays 802.1X client authentication information for all interfaces.

Examples

Display 802.1X client authentication information on GigabitEthernet 1/0/1.

```
<Sysname> display dot1x supplicant interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1
  Username             : aaa
  EAP method           : PEAP-MSCHAPv2
  Dot1x supplicant     : Enabled
  Anonymous identifier : bbb
  SSL client policy    : policy_1
  FSM state            : Init
  EAPOL-Start packets  : 0
```

Table 2 Command output

Field	Description
Username	802.1X client username.
EAP method	802.1X client EAP authentication method: • MD5. • PEAP-GTC. • PEAP-MSCHAPv2. • TTLS-GTC. • TTLS-MSCHAPv2.
Dot1x supplicant	Status of the 802.1X client feature: • Enabled. • Disabled.
Anonymous identifier	802.1X client anonymous identifier.
SSL client policy	SSL client policy used by the 802.1X client feature.

Field	Description
FSM state	802.1X client authentication state: • **Init**—The authentication process starts. • **Connecting**—The 802.1X client is connecting to the authenticator. • **Authenticating**—The 802.1X client is being authenticated. • **Authenticated**—The 802.1X client has been authenticated. • **Held**—The 802.1X client is waiting for authentication.
EAPOL-Start packets	Number of sent EAPOL-Start packets.

dot1x supplicant anonymous identify

Use **dot1x supplicant anonymous identify** to configure an 802.1X client anonymous identifier.

Use **undo dot1x supplicant anonymous identify** to restore the default.

Syntax

dot1x supplicant anonymous identify *identifier*

undo dot1x supplicant anonymous identify

Default

No 802.1X client anonymous identifier exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

identifier: Specifies an 802.1X client anonymous identifier, a case-sensitive string of 1 to 253 characters.

Usage guidelines

At the first authentication phase, packets sent to the authenticator are not encrypted. The use of an 802.1X client anonymous identifier prevents the 802.1X client username from being disclosed at the first phase. The 802.1X client-enabled device sends the anonymous identifier to the authenticator instead of the 802.1X client username. The 802.1X client username will be sent to the authenticator in encrypted packets at the second phase.

If no 802.1X client anonymous identifier is configured, the device sends the 802.1X client username in the first phase.

The configured 802.1X client anonymous identifier takes effect only if one of the following EAP authentication methods is used:

- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

If the MD5-Challenge EAP authentication is used, the configured 802.1X client anonymous identifier does not take effect. The device uses the 802.1X client username at the first authentication phase.

Do not configure the 802.1X client anonymous identifier if the vendor-specific authentication server cannot identify anonymous identifiers.

Examples

Configure the 802.1X client anonymous identifier as **bbb** on a port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant username

dot1x supplicant eap-method

Use **dot1x supplicant eap-method** to specify an 802.1X client EAP authentication method.

Use **undo dot1x supplicant eap-method** to restore the default.

Syntax

dot1x supplicant eap-method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo dot1x supplicant eap-method

Default

The MD5-Challenge authentication is used as the 802.1X client EAP authentication method.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge EAP authentication method.

peap-gtc: Specifies the PEAP-GTC EAP authentication method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 EAP authentication method

ttls-gtc: Specifies the TTLS-GTC EAP authentication method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 EAP authentication method.

Usage guidelines

Make sure the specified 802.1X client EAP authentication method is supported by the authentication server.

Examples

Specify PEAP-GTC as the 802.1X client EAP authentication method on a port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-gtc
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant enable

Use **dot1x supplicant enable** to enable the 802.1X client feature.

Use **undo dot1x supplicant enable** to disable the 802.1X client feature.

Syntax

dot1x supplicant enable

undo dot1x supplicant enable

Default

The 802.1X client feature is disabled.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

Make sure you have configured 802.1X authentication on the authenticator before you use this command.

Examples

Enable the 802.1X client feature on a port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant enable
```

Related commands

display dot1x supplicant

dot1x supplicant mac-address

Use **dot1x supplicant mac-address** to configure an 802.1X client MAC address used for 802.1X client authentication.

Use **undo dot1x supplicant mac-address** to restore the default.

Syntax

dot1x supplicant mac-address *mac-address*

undo dot1x supplicant mac-address

Default

An Ethernet interface uses the interface's MAC address for 802.1X client authentication. If the interface's MAC address is unavailable, the interface uses the device's MAC address for 802.1X client authentication.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses. When entering a MAC address, you can omit the leading zeros in each H section. For example, enter f-e2-1 for 000f-00e2-0001.

Usage guidelines

When the device acts as an 802.1X client and has multiple Ethernet interfaces to seek MACsec protection, each interface requires a unique MAC address to pass 802.1X client authentication.

You can use either of the following methods to configure a unique MAC address for each 802.1X client-enabled interface:

- Execute the **mac-address** command in Ethernet interface view.
- Execute the **dot1x supplicant mac-address** command.

For information about MACsec, see *Security Configuration Guide*.

Examples

Configure the 802.1X client MAC address for 802.1X client authentication as 0001-0001-0001.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant mac-address 1-1-1
```

dot1x supplicant password

Use **dot1x supplicant password** to set an 802.1X client password.

Use **undo dot1x supplicant password** to restore the default.

Syntax

dot1x supplicant password { **cipher** | **simple** } *string*

undo dot1x supplicant password

Default

No 802.1X client password exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 127 characters. Its encrypted form is a case-sensitive string of 1 to 201 characters.

Examples

Set the 802.1X client password to **123456** in plaintext form on a port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

Related commands

display dot1x supplicant

dot1x supplicant enable

dot1x supplicant ssl-client-policy

Use **dot1x supplicant ssl-client-policy** to specify an SSL client policy for an 802.1X client-enabled device.

Use **undo dot1x supplicant ssl-client-policy** to restore the default.

Syntax

dot1x supplicant ssl-client-policy *policy-name*

undo dot1x supplicant ssl-client-policy *policy-name*

Default

An 802.1X client-enabled device uses the default SSL client policy.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-insensitive string of 1 to 31 characters. Make sure the specified SSL client policy already exists.

Usage guidelines

If the PEAP-MSCHAPv2, PEAP-GTC, TTLS-MSCHAPv2, or TTLS-GTC authentication is used, the 802.1X client authentication process is as follows:

- **The first phase**—The device acts as an SSL client to negotiate with the SSL server.

  The SSL client uses the SSL parameters specified in the specified SSL client policy to establish a connection to the SSL server for negotiation. The SSL parameters include a PKI domain, supported cipher suites, and the SSL version. For information about SSL client policies, see *Security Configuration Guide*.
- **The second phase**—The device uses the negotiated result to encrypt and transmit the interchanged authentication packets.

If the MD5-Challenge authentication is used, the device does not use an SSL client policy during the authentication process.

Examples

#Specify SSL client policy **policy_1** to be used by an 802.1X client-enabled device on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant ssl-client-policy policy_1
```

Related commands

display dot1x supplicant

dot1x supplicant enable

ssl client-policy

dot1x supplicant username

Use **dot1x supplicant username** to configure an 802.1X client username.

Use **undo dot1x supplicant username** to restore the default.

Syntax

dot1x supplicant username *username*

undo dot1x supplicant username

Default

No 802.1X client username exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

username: Specifies the 802.1X client username, a case-sensitive string of 1 to 253 characters.

Usage guidelines

802.1X client usernames can include domain names. The supported domain name delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of *username*@*domain-name*, *domain-name**username*, *username*.*domain-name*, or *username*/*domain-name*.

If you want to use backslash (\) as the domain name delimiter, you must enter the escape character (\) along with the backslash (\) sign.

If a username string includes multiple configured delimiters, the device takes the rightmost delimiter in the username string as the domain name delimiter. For more information about the domain name delimiters, see the **dot1x domain-delimiter** command.

Examples

Configure the 802.1X client username as **aaa** on a port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant username aaa
```

Related commands

display dot1x supplicant

dot1x domain-delimiter

dot1x supplicant enable

New feature: MAC address information display for MAC authentication users in MAC authentication VLANs of a specific type

Displaying MAC address information of MAC authentication users in MAC authentication VLANs of a specific type

Execute **display** commands in any view.

Task	Command
Display MAC address information of MAC authentication users in MAC authentication VLANs of a specific type.	**display mac-authentication mac-address** { **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Command reference

display mac-authentication mac-address

Use **display mac-authentication mac-address** to display MAC address information of MAC authentication users in MAC authentication VLANs of a specific type.

Syntax

display mac-authentication mac-address { **critical-vlan** | **guest-vlan** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

critical-vlan: Specifies the MAC authentication critical VLAN.

guest-vlan: Specifies the MAC authentication guest VLAN.

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MAC address information of MAC authentication users in the specified MAC authentication VLAN on all ports.

Usage guidelines

This command displays rough statistics. It might not fully display the specified information when a large number of MAC authentication users perform authentication frequently.

Examples

Display MAC address information of MAC authentication users in the MAC authentication guest VLAN on all ports.

```
<Sysname> display mac-authentication mac-address guest-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1        Guest VLAN: 3          Aging time: N/A
```

```
MAC addresses: 8
  0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
  0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2        Guest VLAN: 5            Aging time: 30 sec
MAC addresses: 2
  0801-2700-9427    0801-2700-2341
```

Table 3 Command output

Field	Description
Total MAC addresses	Total number of MAC addresses in the specified VLAN on the specified port or all ports.
Interface	Access port of MAC authentication users.
Type VLAN	VLAN information for MAC authentication users. The *Type* argument has the following values: • Critical VLAN. • Guest VLAN.
Aging time	MAC address aging time in seconds. This field displays **N/A** if the MAC addresses do not age out.
MAC addresses	Number of matching MAC addresses on a port.
xxxx-xxxx-xxxx	MAC address.

Related commands

mac-authentication critical vlan

mac-authentication guest-vlan

Modified feature: Configuring the hash seed for global link aggregation load sharing

Feature change description

The value range for the hash seed was modified for global link aggregation load sharing.

Command changes

Modified command: link-aggregation global load-sharing seed

Syntax

link-aggregation global load-sharing seed *seed-number*

undo link-aggregation global load-sharing seed

Views

System view

Change description

Before modification: The value range for the *seed-number* argument is 1 to 7FFFFFFF.

After modification: The value range for the *seed-number* argument is 1 to FFFFFFFF.

Modified feature: Specifying a RADIUS or HWTACACS server

Feature change description

Support for specifying a RADIUS or HWTACACS server by its host name was added.

Command changes

Modified commands in RADIUS scheme view: primary accounting, primary authentication, secondary accounting, secondary authentication, state secondary

Old syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

state secondary { **accounting** | **authentication** } [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }

New syntax

primary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

primary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

secondary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo secondary accounting [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo secondary authentication [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

state secondary { **accounting** | **authentication** } [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }

Views

RADIUS scheme view

Change description

The *host-name* argument was added. This argument specifies a RADIUS server by its host name.

Modified commands in HWTACACS scheme view: primary accounting, primary authentication, primary authorization, secondary accounting, secondary authentication, secondary authorization

Old syntax

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

primary authorization { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* I **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authorization { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* I **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authorization [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

New syntax

primary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

primary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

primary authorization { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

secondary accounting { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary accounting [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authentication { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* I **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authentication [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

secondary authorization { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* I **key** { **cipher** | **simple** } *string* | **single-connection**] *

undo secondary authorization [{ *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *]

Views

HWTACACS scheme view

Change description

The *host-name* argument was added. This argument specifies an HWTACACS server by its host name.

Release 3207

This release has the following changes:

- New features: Fundamentals features
- New features: IRF features
- New features: Layer 2—LAN switching features
- New features: Layer 3—IP services features
- New features: Layer 3—IP routing features
- New features: IP multicast features
- New features: ACL and QoS features
- New features: Security features
- New features: High availability features
- New features: Network management and monitoring features
- New features: OpenFlow features
- Modified feature: Configuring a command alias
- Modified feature: Displaying command aliases
- Modified feature: Configuring a hotkey
- Modified feature: Maximum length for a configuration file name
- Modified feature: BFD MAD collision handling process
- Modified feature: Support for commands on IRF physical interfaces
- Modified feature: Excluding a service interface from the IRF MAD shutdown action by the system
- Modified feature: Displaying information about packets dropped on an interface
- Modified feature: Displaying MAC address move records
- Modified feature: MAC address move notifications
- Modified feature: Setting the voice VLAN aging timer
- Modified feature: Creating a VLAN
- Modified feature: Displaying history about ports that are blocked by spanning tree protection features
- Modified feature: Setting the LLDP frame transmission interval
- Modified feature: Displaying ARP entries
- Modified feature: Displaying the aging time of dynamic ARP entries
- Modified feature: Default source IP address in packets relayed to the DHCP server
- Modified feature: Specifying gateways on the DHCP server for DHCP clients
- Modified feature: Displaying information for DHCP snooping trusted ports
- Modified feature: Setting the MTU of IPv4 packets sent over an interface
- Modified feature: Setting the TCP buffer size
- Modified feature: Configuring prefix to be advertised in RA messages
- Modified feature: Setting the MTU of IPv6 packets sent over an interface
- Modified feature: Displaying PBR configuration
- Modified feature: Displaying IPv6 PBR configuration
- Modified feature: Creating an ACL

New features: Fundamentals features

Table 1 describes the fundamental features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Fundamentals Configuration Guide-R3207* and *HPE 5130 EI Switch Series Fundamentals Command Reference-R3207*.

Table 1 Fundamentals features added in version R3207

Feature	Command changes
CLI: Repeating commands in the command history buffer for the current CLI session	The **repeat** [**number**] [**count times**] [**delay seconds**] command was added.
Login management: Associating a Telnet redirect listening port with an IP address	The **ip alias** command was added.
Login management: Specifying an ACL by its name to apply the ACL to the HTTP or HTTPS service	The **name** *acl-name* option was added to the following commands: • **ip http acl** • **ip https acl**
Login management: Enabling RESTful access	The following commands were added: • **restful http enable** • **restful https enable**
Login management: Setting the user line locking key	The **lock-key** *key-string* command was added.
Login management: Locking the current user line and enabling unlocking authentication	The **lock reauthentication** command was added.
Login management: Specifying a source IPv6 address or source interface for outgoing Telnet packets	The **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* } option was added to the **telnet ipv6** command.
Login management: Enabling logging for Telnet login attempts that are denied by the Telnet login control ACL	The **telnet server acl-deny-log enable** command was added.
Login management: Applying a Layer 2 ACL to filter Telnet logins	The **mac** keyword was added to the following commands: • **telnet server ipv6 acl** • **telnet server acl**
Login management: Enabling Web operation logging	The **webui log enable** command was added.
FTP: Enabling logging for FTP login attempts that are denied by the FTP login control ACL	The **ftp server acl-deny-log enable** command was added.
FTP: Associating an SSL server policy with the FTP server	The **ftp server ssl-server-policy** command was added.
Configuration file management: Committing the settings configured after the configuration commit delay timer was set	The **configuration commit** command was added.
Configuration file management: Starting the configuration commit delay timer	The **configuration commit delay** *delay-time* command was added.
Configuration file management: Main next-startup configuration file backup to an IPv6 TFTP server or download from an IPv6 TFTP server	The **ipv6** *ipv6-server* option was added to the following commands: • **backup startup-configuration** • **restore startup-configuration**
Configuration file management: Displaying all running configuration or the running configuration for an IRF member	The **all** and **slot** *slot-number* options were added to the **display current-configuration** command.

Feature	Command changes
device	
Configuration file management: Displaying all running configuration in the current view	The **all** keyword was added to the **display this** command.
Configuration file management: Overwriting the target configuration file with the running configuration if an inconsistency is detected between the settings	The **changed** keyword was added to the **save** command.
Software upgrade: Installing or uninstalling feature or patch images	The following commands were added: • **display install active** • **display install committed** • **install activate** • **install commit** • **install deactivate**
Device management: Displaying CPU usage statistics in table form	The **summary** keyword was added to the **display cpu-usage** command.
Device management: Displaying flash memory information	The **flash** keyword was added to the **display device** command.
Device management: Displaying brief memory usage information	The **summary** keyword was added to the **display memory** command.
Device management: Displaying system stability and status information	The **display system stable state** command was added.
Device management: Setting free-memory thresholds in percentage, and setting and displaying free-memory early-warning thresholds and sufficient-memory thresholds	• The **early-warning**, **secure**, and **ratio** options were added to the **memory-threshold** command. • The **display memory-threshold** command also displays early warning thresholds.

New features: IRF features

Table 2 describes the IRF features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series IRF Configuration Guide-R3207* and *HPE 5130 EI Switch Series IRF Command Reference-R3207*.

Table 2 IRF features added in version R3207

Feature	Command changes
Bulk-configuring basic IRF settings	The **easy-irf** command was added.

New features: Layer 2—LAN switching features

Table 3 describes the Layer 2—LAN switching features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Layer 2—LAN Switching Configuration Guide-R3207* and *HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207*.

Table 3 Layer 2—LAN switching features added in version R3207

Feature	Command changes
Ethernet link aggregation: Configuring an aggregate interface as an edge aggregate interface	The **lacp edge-port** command was added.
Ethernet link aggregation: Configuring LACP to operate in passive mode on a port	The **lacp mode passive** command was added.
Ethernet link aggregation: Using the port speeds as the preferential criteria for selecting a reference port for a dynamic aggregation group	The **lacp select speed** command was added.
Ethernet link aggregation: Enabling the current interface to synchronize the attribute configurations from the aggregate interface when the interface was assigned to the aggregate interface	The **force** keyword was added to the **port link-aggregation group** command.
Spanning tree: Enabling SNMP notifications for new-root election events or spanning tree topology changes	The **new-root** and **tc** keywords were added to the **snmp-agent trap enable stp** command.
Spanning tree: Enabling dispute guard	The **stp dispute-protection** command was added.
Spanning tree: Disabling inconsistent PVID protection	The **stp ignore-pvid-inconsistency** command was added.
Spanning tree: Configuring BPDU guard on an interface	The **stp port bpdu-protection** { **enable** | **disable** } command was added.
Spanning tree: Disabling the device from reactivating edge ports shut down by BPDU guard	The **stp port shutdown permanent** command was added.
Spanning tree: Enabling PVST BPDU guard	The **stp pvst-bpdu-protection** command was added.
VLAN: Clearing statistics on a VLAN interface	The **reset counters interface vlan-interface**
VLAN: Associating a VLAN with the specified protocol template	The **raw** keyword was added to the **protocol-vlan** command.
L2PT: Enabling L2PT for UDLD	The **udld** keyword was added to the **l2protocol tunnel dot1q** command.
LLDP: Enabling advertisement of the management address TLV globally and setting the management address to be advertised	The **lldp** [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-enable basic-tlv management-address-tlv** [**ipv6**] { *ip-address* | **interface loopback** *interface-number* | **interface vlan-interface** *interface-number* } command was added.

New features: Layer 3—IP services features

Table 4 describes the Layer 3—IP services features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Layer 3—IP Services*

Configuration Guide-R3207 and *HPE 5130 EI Switch Series Layer 3—IP Services Command Reference-R3207*.

Table 4 Layer 3—IP services features added in version R3207

Feature	Command changes
Displaying the maximum number of ARP entries that a device supports	The **display arp entry-limit** command was added.
Setting the aging timer for dynamic ARP entries	The **second** *aging-seconds* option was added to the **arp timer aging** command.
Setting the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change	The **gratuitous-arp mac-change retransmit** *times* **interval** *seconds* command was added.
IP addressing: Displaying brief IP configuration for Layer 3 interfaces	The **description** keyword was added to the **display ip interface brief** command.
Enabling client offline detection on the DHCP server or relay agent	The **dhcp client-detect** command was added.
Enabling DHCP logging on the DHCP server	The **dhcp log enable** command was added.
Enabling the DHCP server proxy on the relay agent	The **proxy** keyword was added to the **dhcp select** command.
DHCP server: Specifying a DHCP address pool for a DHCP user class	The **class ip-pool** command was added.
DHCP server: Specifying a DHCP option group for a DHCP user class in a DHCP address pool	The **class option-group** command was added.
DHCP server: Specifying the default DHCP address pool	The **default ip-pool** command was added.
DHCP server: Applying a DHCP policy to an interface	The **dhcp apply-policy** command was added.
DHCP server: Creating a DHCP option group and entering its view	The **dhcp option-group** command was added.
DHCP server: Creating a DHCP policy	The **dhcp policy** command was added.
DHCP server: Enabling MAC address check on the DHCP server.	The **dhcp server check mac-address** command was added.
DHCP server: Configuring the DHCP server to back up the bindings to a file	The following commands were added: • **dhcp server database filename** • **dhcp server database update interval** • **dhcp server database update now** • **dhcp server database update stop** • **display dhcp server database**
DHCP server: Configuring a match rule for a DHCP user class	The following parameters were added to the **if-match** command: • **hardware-address** *hardware-address* • **mask** *hardware-address-mask* • **ascii** *ascii-string* • **offset** *offset* • **partial**

Feature	Command changes
	• **relay-agent** *gateway-address*
DHCP server: Setting the DHCP address pool usage threshold	The **ip-in-use threshold** command was added.
DHCP server: Customizing a DHCP option	The **option** command was added in DHCP option group view.
DHCP server: Configuring the DHCP server in DHCP policy view	The following commands were added in DHCP policy view: • **class ip-pool** • **default ip-pool**
DHCP server: Adding DHCP user classes to the whitelist	The **valid class** command was added.
DHCP server: Enabling the DHCP user class whitelist	The **verify class** command was added.
DHCP relay agent: Setting the DHCP server response timeout time for DHCP server switchover	The **dhcp relay dhcp-server timeout** command was added.
DHCP relay agent: Specifying the DHCP relay agent address to be inserted in DHCP requests	The **dhcp relay gateway** command was added.
DHCP relay agent: Configuring the padding mode and padding format for the Circuit ID sub-option	The following keywords were added to the **dhcp relay information circuit-id** command: • **bas** • **interface**
DHCP relay agent: Enabling the switchback to the master DHCP server and setting the delay time	The following commands were added: • **dhcp relay master-server switch-delay** • **master-server switch-delay**
DHCP relay agent: Specifying the DHCP server selecting algorithm	The following commands were added: • **dhcp relay server-address algorithm** • **remote-server algorithm**
DHCP relay agent: Specifying the source IP address for relayed DHCP requests	The **dhcp relay source-address** command was added.
DHCP relay agent: Enabling the DHCP smart relay feature	**dhcp smart-relay enable**
DHCP relay agent: Setting the DHCP server response timeout time for DHCP server switchover	The **dhcp-server timeout** command was added.
DHCP relay agent: Specifying DHCP servers for a DHCP address pool	The **remote-server** command was added.
DHCP snooping: Enabling the recording of DHCP snooping entries for a VLAN	The **dhcp snooping binding record** command was added in VLAN view.
DHCP snooping: Disabling DHCP snooping on an interface	The **dhcp snooping disable** command was added.
DHCP snooping: Enabling DHCP snooping for VLANs	The **dhcp snooping enable vlan** command was added.
DHCP snooping: Configuring an interface in a VLAN as a trusted port	The **dhcp snooping trust interface** command was added.

Feature	Command changes
DHCP snooping: Displaying DHCP snooping entries	The **verbose** keyword was added to the **display dhcp snooping binding** command.
IP forwarding basics: Saving the IP forwarding entries to a file	The **ip forwarding-table save filename** *filename* command was added.
IP performance optimization: Enabling an interface to forward directed broadcasts destined for the directly connected network	The **acl** *acl-number* option was added to the **ip forward-broadcast** command.
IPv6 basics: Displaying the maximum number of ND entries that a device supports	The **display ipv6 neighbors entry-limit** command was added.
IPv6 basics: Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address and advertising the prefix	The **ipv6 address** *prefix-number* command was added.
IPv6 basics: Configuring the default settings for prefixes advertised in RA messages	The **ipv6 nd ra prefix default** command was added.
IPv6 basics: Setting the interval for retransmitting an NS message for DAD	The **ipv6 nd snooping dad retrans-timer** *interval* command was added.
IPv6 basics: Setting timeout timers for ND snooping entries	The **ipv6 nd snooping lifetime** { **invalid** *invalid-lifetime* | **valid** *valid-lifetime* } command was added.
IPv6 basics: Configuring the port as an ND snooping uplink port which cannot learn ND snooping entries	The **ipv6 nd snooping uplink** command was added.
IPv6 basics: Enabling IPv6 local fragment reassembly	The **ipv6 reassemble local enable** command was added.
Enabling the DHCPv6 server or relay agent to advertise IPv6 prefixes	The **ipv6 dhcp advertise pd-route** command was added.
Enabling DHCPv6 logging on the DHCPv6 server	The **ipv6 dhcp log enable** command was added.
DHCPv6 server: Specifying a DHCPv6 address pool for a DHCPv6 user class	The **class pool** command was added.
DHCPv6 server: Specifying the default DHCPv6 address pool	The **default pool** command was added.
DHCPv6 server: Displaying information about a DHCPv6 option group	The **display ipv6 dhcp option-group** command was added.
DHCPv6 server: Configuring the DHCPv6 server in DHCPv6 option group view	The following commands were added in DHCPv6 option group view: • **dns-server** • **domain-name**
DHCPv6 server: Configuring a match rule for a DHCPv6 user class	The **if-match** command was added.
DHCPv6 server: Applying a DHCPv6 policy to an interface	The **ipv6 dhcp apply-policy** command was added.
DHCPv6 server: Creating a DHCPv6 user	The **ipv6 dhcp class** command was added.

Feature	Command changes
class and entering DHCPv6 user class view	
DHCPv6 server: Creating a static DHCPv6 option group	The **ipv6 dhcp option-group** command was added.
DHCPv6 server: Creating a DHCPv6 policy	The **ipv6 dhcp policy** command was added.
DHCPv6 server: Specifying a prefix for a DHCPv6 address pool	The **prefix** *prefix-number* option was added to the **ipv6 dhcp prefix-pool** command.
DHCPv6 server: Configuring the DHCPv6 server to back up the bindings to a file	The following commands were added: • **ipv6 dhcp server database filename** • **ipv6 dhcp server database update interval** • **ipv6 dhcp server database update now** • **ipv6 dhcp server database update stop** • **display ipv6 dhcp server database**
DHCPv6 server: Specifying an IPv6 subnet for dynamic allocation in a DHCPv6 address pool	The following options were added to the **networ**k command: • **prefix** *prefix-number* • *sub-prefix*/*sub-prefix-length*
DHCPv6 server: Configuring the DHCPv6 server in DHCPv6 option group view	The following commands were added in DHCPv6 option group view: • **option** • **sip-server**
DHCPv6 server: Specifying a DHCPv6 option group for a DHCPv6 address pool	The **option-group** command was added.
DHCPv6 relay agent: Displaying DHCPv6 relay entries that record clients' IPv6 address information	The **display ipv6 dhcp relay client-information address** command was added.
DHCPv6 relay agent: Displaying DHCPv6 relay entries that record clients' IPv6 prefix information	The **display ipv6 dhcp relay client-information pd** command was added.
DHCPv6 relay agent: Specifying gateway addresses for DHCPv6 clients in a DHCPv6 address pool	The **gateway-list** command was added.
DHCPv6 relay agent: Enabling client offline detection	The **ipv6 dhcp client-detect** command was added.
DHCPv6 relay agent: Enabling the DHCPv6 relay agent to record relay entries	The **ipv6 dhcp relay client-information record** command was added.
DHCPv6 relay agent: Specifying a gateway address for DHCPv6 clients	The **ipv6 dhcp relay gateway** command was added.
DHCPv6 relay agent: Specifying a padding mode for the Interface-ID option	The **ipv6 dhcp relay interface-id** command was added.
DHCPv6 relay agent: Enabling IPv6 release notification	The **ipv6 dhcp relay release-agent** command was added.
DHCPv6 relay agent: Specifying DHCPv6 servers for the DHCPv6 address pool	The **remote-server** command was added.
DHCPv6 relay agent: Clearing DHCPv6	The **reset ipv6 dhcp relay**

Feature	Command changes
relay entries that record clients' IPv6 address information	**client-information address** command was added.
DHCPv6 relay agent: Clearing DHCPv6 relay entries that record clients' IPv6 prefix information	The **reset ipv6 dhcp relay client-information pd** command was added.
DHCPv6 client: Configuring the interface to use DHCPv6 to obtain an IPv6 address and other configuration parameters	The **option-group** *option-group-number* option was added to the following commands: • **ipv6 dhcp client pd** • **ipv6 address dhcp-alloc**
DHCPv6 client: Configuring the DHCPv6 client DUID	The **ipv6 dhcp client duid** command was added.
DHCPv6 client: Configuring the interface to use DHCPv6 to obtain an IPv6 address, an IPv6 prefix, and other configuration parameters	The **ipv6 dhcp client stateful** command was added.

New features: Layer 3—IP routing features

Table 5 describes the Layer 3—IP routing features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Layer 3—IP Routing Configuration Guide-R3207* and *HPE 5130 EI Switch Series Layer 3—IP Routing Command Reference-R3207.*

Table 5 Layer 3—IP routing features added in version R3207

Feature	Command changes
RIP: Displaying the GR status for a RIP process	The **display rip graceful-restart** command was added.
RIP: Displaying the NSR status for a RIP process	The **display rip non-stop-routing** command was added.
RIP: Setting the GR interval	The **graceful-restart interval** command was added.
RIP: Enabling RIP NSR	The **non-stop-routing** command was added.
RIP: Configuring RIP FRR	The **fast-reroute** command was added.
RIPng: Displaying the GR status for a RIPng process	**The display ripng graceful-restart command was added.**
RIPng: Displaying the NSR status for a RIPng process	**The display ripng non-stop-routing command was added.**
RIPng: Enabling RIPng FRR	**The fast-reroute command was added.**
RIPng: Setting the GR interval	The **graceful-restart interval** command was added.
RIPng: Enabling RIPng NSR	The **non-stop-routing** command was added.
RIPng: Enabling BFD single-hop echo detection for RIPng FRR	The **ripng primary-path-detect bfd echo** command was added.

New features: IP multicast features

Table 6 describes the IP multicast features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series IP Multicast Configuration Guide-R3207* and *HPE 5130 EI Switch Series IP Multicast Command Reference-R3207*.

Table 6 IP multicast features added in version R3207

Feature	Command changes
IGMP snooping: Displaying information about dynamic IGMP snooping group entries for an interface	The **interface** *interface-type interface-number* option was added to the **display igmp-snooping group** command.
IGMP snooping: Displaying detailed information about dynamic router ports	The **verbose** keyword was added to the **display igmp-snooping router-port** command.
IGMP snooping: Displaying detailed information about static router ports	The **verbose** keyword was added to the **display igmp-snooping static-router-port** command.
IGMP snooping: Enabling IGMP snooping globally	The **global-enable** command was added.
IGMP snooping: Disabling IGMP snooping for a VLAN	The **igmp-snooping disable** command was added.
PIM snooping: Displaying detailed information about PIM snooping router ports	The **verbose** keyword was added to the **display pim-snooping router-port** command.
MLD snooping: Displaying information about dynamic MLD snooping group entries for an interface	The **interface** *interface-type interface-number* option was added to the **display mld-snooping group** command.
MLD snooping: Displaying detailed information about dynamic router ports	The **verbose** keyword was added to the **display mld-snooping router-port** command.
MLD snooping: Displaying detailed information about static router ports	The **verbose** keyword was added to the **display mld-snooping static-router-port** command.
MLD snooping: Enabling MLD snooping globally	The **global-enable** command was added.
MLD snooping: Disabling MLD snooping for a VLAN	The **mld-snooping disable** command was added.
IPv6 PIM snooping: Displaying detailed information about IPv6 PIM snooping router ports	The **verbose** keyword was added to the **display ipv6 pim-snooping router-port** command.

New features: ACL and QoS features

Table 7 describes the ACL and QoS features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series ACL and QoS Configuration Guide-R3207* and *HPE 5130 EI Switch Series ACL and QoS Command Reference-R3207*.

Table 7 ACL and QoS features added in version R3207

Feature	Command changes
ACL: Enabling SNMP notifications for packet filtering and setting the interval	The **acl trap interval** command was added.
ACL: Setting a rule numbering step for an ACL	The **start** *start-value* option was added to the **step** command.
QoS: Configuring a description for a traffic class	The **description** command was added.
QoS: Associating a traffic behavior with a traffic class in a QoS policy	The **insert-before** *before-classifier-name* option was added to the **classifier behavior** command.
QoS: Displaying QoS policies applied to user profiles	**display qos policy user-profile**
QoS: Configuring queue scheduling profiles	The following commands were added: • **display qos qmprofile configuration** • **display qos qmprofile interface** • **qos qmprofile** • **bandwidth queue** • **queue** • **qos apply qmprofile**
Data buffer: Configuring data buffer monitoring	The following commands were added: • **display buffer usage interface** • **buffer usage threshold**

New features: Security features

Table 8 describes the security features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Security Configuration Guide-R3207* and *HPE 5130 EI Switch Series Security Command Reference-R3207*.

Table 8 Security features added in version R3207

Feature	Command changes
AAA: New authorization attributes for users	The following parameters were added in the **authorization-attribute** command in ISP domain view: • **acl** • **car** • **igmp**

Feature	Command changes
	• **mld** • **url** • **user-group** The following parameters were added in the **authorization-attribute** command in local user view or user group view: • **idle-cut** • **session-timeout**
AAA: Configuring the device to include the idle cut period in the user online duration sent to the server	The **session-time include-idle-time** command was added.
AAA: Configuring a description for a network access user	The **description** command was added in local user view.
AAA: Configuring the auto-delete feature of local users	The **local-user auto-delete enable** command was added.
AAA: Configuring the validity period for a network access user	The **validity-datetime** command was added.
AAA: Configuring the device ID	The **aaa device-id** command was added.
AAA: Enabling the extended accounting-on feature	The **accounting-on extended** command was added.
AAA: Configuring the device to interpret the RADIUS class attribute (attribute 25) as CAR parameters	The **attribute 25 car** command was added.
AAA: Configuring the MAC address format for RADIUS attribute 31	The **attribute 31 mac-format** command was added.
AAA: Setting the data measurement unit for the Remanent_Volume attribute	The **attribute remanent-volume** command was added.
AAA: Configuring the RADIUS attribute translation feature	The following commands were added: • **attribute convert** (RADIUS DAS view) • **attribute convert** (RADIUS scheme view) • **attribute reject** (RADIUS DAS view) • **attribute reject** (RADIUS scheme view) • **attribute translate** • **radius attribute extended**
AAA: Configuring the DSCP priority of RADIUS packets	The **radius dscp** command was added.
AAA: Support for CoA messages to shut down or reboot the access port of users or reauthenticate users	N/A
AAA: Specifying a RADIUS session-control client	The **radius session-control client** command was added.
AAA: Configuring an LDAP attribute map	The following commands were added: • **attribute-map** • **ldap attribute-map** • **map**

Feature	Command changes
AAA: Specifying the LDAP authorization server	The **authorization-server** command was added.
AAA: Broadcasting RADIUS accounting requests	The **broadcast** keyword was added to the following commands: • **accounting lan-access** • **accounting portal**
AAA: Displaying the HWTACACS service statistics	The **display hwtacacs scheme** [*hwtacacs-scheme-name* **statistics**] command was added.
AAA: Configuring the RADIUS server feature	The following commands were added: • **display radius-server active-client** • **display radius-server active-user** • **radius-server activate** • **radius-server client**
AAA: Support for RADIUS attribute 168 (Framed-IPv6-Address) to accept the IPv6 addresses assigned by the server to hosts	N/A
802.1X: Redirect URL assignment	N/A
802.1X: Displaying information about online 802.1X open users	The **open** keyword was added to the **display dot1x connection** command.
802.1X: Displaying MAC address information of 802.1X users in specific VLANs	The **display dot1x mac-address** command was added.
802.1X: Enabling logging for 802.1X users	The **dot1x access-user log enable** command was added.
802.1X: Setting the maximum number of 802.1X authentication attempts for MAC authenticated users	The **dot1x after-mac-auth max-attempt** command was added.
802.1X: Specifying supported domain name delimiters	The **dot1x domain-delimiter** command was added.
MAC authentication: Redirect URL assignment	N/A
MAC authentication: Displaying information about online MAC authentication open users	The **open** keyword was added to the **display mac-authentication connection** command.
MAC authentication: Displaying MAC address information of MAC authentication users in specific VLANs	The **display mac-authentication mac-address** command was added.
MAC authentication: Enabling logging for MAC authentication users	The **mac-authentication access-user log enable** command was added.
MAC authentication: Enabling the authorization VLAN auto-tag feature	The **mac-authentication auto-tag** [**ignore-config**] command was added.
MAC authentication: Including user IP addresses in MAC authentication requests	The **mac-authentication carry user-ip** command was added.
Port security: Redirect URL assignment for	N/A

Feature	Command changes
specific port security modes	
Port security: Enabling open authentication mode	The following commands were added: • **port-security authentication open** • **port-security authentication open global**
Port security: Setting the secure MAC aging timer in seconds	The **second** keyword was added to the **port-security timer autolearn aging** command.
Port security: Enabling logging for port security users	The **port-security access-user log enable** command was added.
Port security: Enabling the quiet timer function for the authorization-fail-offline feature	The **quiet-period** keyword was added to the **port-security authorization-fail offline** command.
Port security: Setting port security's limit on the number of MAC addresses for specific VLANs on a port	The **port-security mac-limit** command was added.
Port security: Setting port security's limit on the number of secure MAC addresses for specific VLANs on a port	The **vlan** [*vlan-id-list*] option was added to the **port-security max-mac-count** command.
Portal support for EAP	N/A
Portal: Displaying information about portal users	The following parameters were added in the **display portal user** command: • **ip** • **ipv6** • **pre-auth** • **verbose**
Portal: Displaying information about Web redirect rules	The **display web-redirect rule interface** *interface-type interface-number* [**slot** *slot-number*] command was added.
Portal: Configuring a match rule for URL redirection	The **if-match** { **original-url** *url-string* **redirect-url** *url-string* [**url-param-encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **user-agent** *string* **redirect-url** *url-string* } command was added.
Portal: Setting the maximum number of portal users on an interface	The **portal** { **ipv4-max-user** | **ipv6-max-user** } *max-number* command was added.
Portal: Enabling strict checking on portal authorization information	The **portal authorization** { **acl** | **user-profile** } **strict-checking** command was added.
Portal: Specifying the Layer 3 interface on which an IP-based portal-free rule takes effect	The **interface** *interface-type interface-number* option was added to the **portal free-rule** command.

Feature	Command changes
Portal: Configuring a destination-based portal-free rule	The **portal free-rule** *rule-number* **destination** *host-name* command was added.
Portal: Enabling logging for portal logins and logouts	The **portal log enable** command was added.
Portal: Specifying the format for the NAS-Port-Id attribute	The **portal nas-port-id format** { **1** | **2** | **3** | **4** } command was added.
Portal: Specifying a portal preauthentication domain	The **portal** [**ipv6**] **pre-auth domain** *domain-name* command was added.
Portal: Enabling the Rule ARP or ND entry feature for portal clients	The **portal refresh** { **arp** | **nd** } **enable** command was added.
Portal: Allowing only users with DHCP-assigned IP addresses to pass portal authentication	The **portal** [**ipv6**] **user-dhcp-only** command was added.
Portal: Specifying the port number of a Web proxy server	The **portal web-proxy port** *port-number* command was added.
Portal: Configuring the device to periodically register with the portal authentication server	The **server-register** [**interval** *interval-value*] command was added.
Portal: Specifying the type of a portal authentication server or portal Web server	The **server-type** { **cmcc** | **imc** } command was added.
Portal: Configuring the device to carry the user MAC address in encrypted form in the redirect URL	The [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] parameter was added to the **url-parameter** command.
Portal: Configuring Web redirect	The **web-redirect** [**ipv6**] **url** *url-string* [**interval** *interval*] command was added.
Web authentication: Setting the redirection wait time	The **redirect-wait-time period** command was added.
Web authentication: Adding parameters to the redirection URL of the Web authentication server	The **url-parameter parameter-name** { **original-url** | **source-address** | **source-mac** | **value expression** } command was added.
PKI: Specifying an ECDSA key pair for certificate request	The **public-key ecdsa name** *key-name* [**secp256r1** | **secp384r1** | **secp521r1**] command was added in FIPS mode.
IKE: Configuring a description for an IKE proposal	The **description** *text* command was added.
IKE: Displaying IKE statistics	The **display ike statistics** command was added.
IKEv2: Displaying IKEv2 statistics	The **display ikev2 statistics** command was added.
IKEv2: Clearing IKEv2 statistics	The **reset ikev2 statistics** command was added.
SSL: SSL server support for optional SSL client authentication	The **optional** keyword was added to the **client-verify** command.
SSL: Setting the timeout time for cached sessions	The **timeout** *time* option was added to the

Feature	Command changes
	session command.
SSH: Releasing SSH connections	The **free ssh** { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* } command was added.
SSH: Enabling logging for SSH login attempts that are denied by the SSH login control ACL	The **ssh server acl-deny-log enable** command was added.
SSH: Specifying the SSH service port	The **ssh server port** *port-number* command was added.
SSH: Deleting server public keys saved in the public key file on the SSH client	The **delete ssh client server-public-key** [**server-ip** *ip-address*] command was added.
SSH: Displaying server public key information saved in the public key file of the SSH client	The **display ssh client server-public-key** [**server-ip** *ip-address*] command was added.
802.1X client	All 802.1X client commands were newly added.
IP source guard: Displaying IPv4SG bindings dynamically generated based on ARP snooping or 802.1X	The **arp-snooping** and **dot1x** keywords were added to the **display ip source binding** command.
IP source guard: Displaying IPv6SG bindings dynamically generated based on DHCPv6 relay agent, 802.1X, or ND snooping	The following keywords were added to the **display ipv6 source binding** command: • **dhcpv6-relay** • **dot1x** • **nd-snooping**
ARP attack protection: Converting valid static ARP entries to dynamic ARP entries and deleting invalid static ARP entries	The **undo arp fixup** command was added.
ARP attack protection: Specifying the sender IP address range for ARP packet checking	The **arp sender-ip-range** command was added.
SAVI	All SAVI commands were newly added.

New features: High availability features

Table 9 describes the high availability features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series High Availability Configuration Guide-R3207* and *HPE 5130 EI Switch Series High Availability Command Reference-R3207*.

Table 9 High availability features added in version R3207

Feature	Command changes
CFD: Enabling two-way DM	The **dot1p** *dot1p-value* and **interval** *interval* options were added to the **cfd dm two-way** command.
CFD: Enabling loss measurement	The **dot1p** *dot1p-value* and **interval** *interval* options were added to the **cfd slm** command.
DLDP: Setting the port shutdown mode	The **hybrid** keyword was added to the **dldp**

Feature	Command changes
	unidirectional-shutdown command.
BFD: Creating a BFD session for detecting the local interface state	The **bfd detect-interface source-ip** command was added.
BFD: Enabling the echo packet mode	The **receive** and **send** keywords were added to the **bfd echo enable** command.
BFD: Enabling SNMP notifications for BFD	The **snmp-agent trap enable bfd** command was added.
Monitor Link: Configuring the uplink interface threshold for triggering monitor link group state switchover	The **uplink up-port-threshold** command was added.
Process placement	All process placement commands were newly added.
Track: Displaying track entry information	The **negative**, **positive**, and **brief** keywords were added to the **display track** command.
Track: Creating a track entry and associate it with the physical state of an interface	The **track interface physical** command was added.
Track: Creating a track entry and associate it with a route entry	The **track ip route reachability** command was added.
Track: Creating a track entry and associate it with the neighbor availability status of an LLDP interface	The **track lldp neighbor** command was added.

New features: Network management and monitoring features

Table 10 describes the network management and monitoring features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series Network Management and Monitoring Configuration Guide-R3207 and HPE 5130 EI Switch Series Network Management and Monitoring Command Reference-R3207*

Table 10 Network management and monitoring features added in version R3207

Feature	Command changes
NQA: Specifing a community name for the SNMP operation	The **community read** command was added.
NQA: Specifying a destination device by its host name for the UDP tracert operation	The **destination host** command was added.
NQA: Configuring the RADIUS template	The **key** command was added.
NQA: Specifying the next hop IP address for ICMP echo requests	The **next-hop** command was added
NQA: Configuring the TCP half open template	N/A
NQA: Configuring the SSL template	The **ssl-client-policy** command was added.
NQA: Configuring the HTTPS template	N/A
NTP: Configuring NTP authentication	The **hmac-sha-1**, **hmac-sha-256**, **hmac-sha-384**, and **hmac-sha-512** keywords

Feature	Command changes
	were added to the **ntp-service authentication-keyid** command.
NETCONF: Specifying a mandatory authentication domain for NETCONF users	The **netconf soap domain** command was added.
NETCONF: Applying an ACL to NETCONF over SOAP traffic	The **netconf soap acl** command was added.
NETCONF: Setting the DSCP value for outgoing NETCONF over SOAP packets	The **netconf soap dscp** command was added/
NETCONF: Specifying a specific name space.	The **netconf capability specific-namespace** command was added.
NETCONF: Setting the NETCONF session idle timeout time	The **netconf idle-timeout** command was added.
NETCONF: Support for the *OverWrite* attribute for saving the running configuration	N/A
NETCONF: Subscribing to monitoring events and module report events	N/A
NETCONF: Retrieving NETCONF information	N/A
NETCONF: Retrieving YANG file content	N/A
NETCONF: Not support for the <edit-config> operation while the device is rolling back configuration.	N/A
VCF fabric	All VCF fabric commands were newly added.
SNMP: Calculating the encrypted form for a key in plaintext form	• In non-FIPS mode: The **aes192md5**, **aes192sha**, **aes256md5**, and **aes256sha** keywords were added to the **snmp-agent calculate-password** command. • In FIPs mode: The **aes192sha** and **aes256sha** keywords were added to the **snmp-agent calculate-password** command.
EAA: Configuring a member device join or leave event	The **insert** and **remove** keywords were added to the **event hotplug** command.
EAA: Configuring a track event for a CLI-defined monitor policy	The **event track** command was added.
EAA: Setting the size for the EAA-monitored log buffer	The **rtm event syslog buffer-size** command was added.
Process monitoring and maintenance: Specifying the action to be taken in response to a kernel thread deadloop	The **monitor kernel deadloop action** command was added.
Process monitoring and maintenance: Enabling kernel thread deadloop detection for a CPU core.	The **core** keyword was added to the **monitor kernel deadloop enable** command.
Information center: Setting the maximum number of log traps that can be stored in the log trap buffer	The **info-center syslog trap** command was added.
Information center: Enabling SNMP notifications for log messages	The **snmp-agent trap enable syslog** command was added.

New features: OpenFlow features

Table 11 describes the OpenFlow features added in this software version. For more information about the features and commands, see *HPE 5130 EI Switch Series OpenFlow Configuration Guide-R3207* and *HPE 5130 EI Switch Series OpenFlow Command Reference-R3207*.

Table 11 OpenFlow features added in version R3207

Feature	Command changes
Displaying information of the client that connects to the server that is enabled for an OpenFlow instance in the controller information	The **listened** keyword was added to the **display openflow** command.
Adding the VLAN tagging and untagging flow tables	The **ingress-vlan** ingress-table-id and **egress-vlan** egress-table-id options were added to the **flow-table** command.
Clearing statistics on packets that a controller sends and receives for an OpenFlow instance	The **reset openflow instance statistics** command was added.
Adding the smart interruption mode	The **smart** keyword was added to the **fail-open mode** command.

Modified feature: Configuring a command alias

Feature change description

The syntax of the command for configuring a command alias changed from **command-alias mapping** to **alias**.

Command changes

Modified command: command-alias mapping

Old syntax

command-alias mapping

New syntax

alias

Views

Any view

Change description

Before modification: The command syntax is **command-alias mapping**.

After modification: The command syntax is **alias**.

Modified feature: Displaying command aliases

Feature change description

The syntax of the command for displaying command aliases changed from **display command-alias** to **display alias**.

Command changes

Modified command: display command-alias

Old syntax

display command-alias

New syntax

display alias

Views

Any view

Change description

Before modification: The command syntax is **display command-alias**.

After modification: The command syntax is **display alias**.

Modified feature: Configuring a hotkey

Feature change description

More hotkeys can be modified.

Command changes

Modified command: hotkey

Old syntax

hotkey { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*

New syntax

hotkey *hotkey* { *command* | **function** *function* | **none** }

Views

System view

Change description

Before modification: The command allows you to configure only five hotkeys.

After modification: The command allows you to configure all hotkeys.

Modified feature: Maximum length for a configuration file name

Feature change description

The maximum length was increased for a configuration file name.

Command changes

Modified command: configuration replace file

Syntax

configuration replace file *filename*

Views

System view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

Modified command: restore startup-configuration

Syntax

restore startup-configuration from *tftp-server src-filename*

Views

User view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

Modified command: save

Syntax

save *file-url* [**all** | **slot** *slot-number*]

Views

Any view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

Modified command: startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

Views

User view

Change description

Before modification: The maximum length cannot exceed 191 characters for a configuration file name. The file name can include the file path.

After modification: The maximum length cannot exceed 255 characters for a configuration file name. The file name can include the file path.

Modified feature: BFD MAD collision handling process

Feature change description

Before modification, BFD MAD uses the following process to handle a multi-active collision:

1. Compares the member IDs of the masters in the split IRF fabrics.
2. Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

BFD MAD cannot be configured together with LACP MAD, because they handle collisions differently.

After modification, BFD MAD uses the following process to handle a multi-active collision:

1. Compares the number of members in each split IRF fabric.
2. Sets all fabrics to the Recovery state except the one that has the most members.
3. Compares the member IDs of the masters if all IRF fabrics have the same number of members.
4. Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

BFD MAD can be configured together with LACP MAD.

Command changes

None.

Modified feature: Support for commands on IRF physical interfaces

Feature change description

The following commands were added on IRF physical interfaces:

- MAC address table configuration commands, including the **mac-address static source-check enable** command. For information about this command, see *HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207*.
- The **mirroring-group reflector-port** command. Use this command to configure the reflector port for a remote source group. When you execute this command on an IRF physical interface, the binding between the physical interface and IRF port is removed. To avoid IRF split, do not configure a physical interface as a reflector port if that interface is the only member

interface of an IRF port. For more information about the **mirroring-group reflector-port** command, see *HPE 5130 EI Switch Series Network Management and Monitoring Command Reference-R3207.*

- LLDP commands, including:
  - **lldp admin-status**
  - **lldp check-change-interval**
  - **lldp enable**
  - **lldp encapsulation snap**
  - **lldp notification remote-change enable**
  - **lldp tlv-enable**

  Use these commands to view the connectivity and status of IRF links. For more information about LLDP commands, see *HPE 5130 EI Switch Series Layer 2—LAN Switching Command Reference-R3207*.

Command changes

The following commands were added in IRF physical interface view:

- **lldp admin-status**
- **lldp check-change-interval**
- **lldp enable**
- **lldp encapsulation snap**
- **lldp notification remote-change enable**
- **lldp tlv-enable**
- **mac-address static source-check enable**
- **mirroring-group reflector-port**

Modified feature: Excluding a service interface from the IRF MAD shutdown action by the system

Feature change description

When the IRF fabric transits to the Recovery state, the system automatically excludes the following service interfaces from being shut down:

- Before modification:
  - IRF physical interfaces.
  - Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.
- After modification:
  - IRF physical interfaces.
  - Interfaces used for BFD MAD.
  - Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.

Command changes

None.

Modified feature: Displaying information about packets dropped on an interface

Feature change description

Statistics about packets dropped due to insufficient data buffer were displayed.

Command changes

Modified command: display packet-drop

Syntax

display packet-drop { **interface** [*interface-type* [*interface-number*]] | **summary** }

Views

Any view

Change description

Before modification: The command cannot display statistics about packets dropped due to insufficient data buffer.

After modification: The command can display statistics about packets dropped due to insufficient data buffer as follows:

```
Packets dropped due to insufficient data buffer. Input dropped: 0 Output dropped:0
```

Modified feature: Displaying MAC address move records

Feature change description

The maximum number of MAC address move records the device can display changed from 20 to 200.

Command changes

None.

Modified feature: MAC address move notifications

Feature change description

Before modification: Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The most recent record will override the oldest one.

After modification:

Within a detection interval, an IRF member device can record MAC address move information for a maximum of 20 MAC addresses. The records are ranked in descending order of MAC move counts. When the MAC move count of a new record is higher than the MAC move count of any existing record, the device performs the following operations:

- Discards the record that has the lowest MAC move count.
- Ranks the MAC address move records in descending order of MAC move count.

Then, in the next detection interval, the device discards all MAC address move records generated in the previous detection interval and starts another round of MAC move record generation.

Command changes

None.

Modified feature: Setting the voice VLAN aging timer

Feature change description

You can configure voice VLANs not to age out in this version and later.

Command changes

Modified command: voice-vlan aging

Syntax

voice-vlan aging *minutes*

undo voice-vlan aging

Views

System view

Change description

Before modification: The value of voice VLAN aging timer is in the range of 5 to 43200 minutes.

After modification: The value of voice VLAN aging timer can be 0 minutes or in the range of 5 to 43200 minutes. If you set the voice VLAN aging timer to 0 minutes, the voice VLAN does not age out.

Modified feature: Creating a VLAN

Feature change description

When you create a VLAN, you can specify a space-separated list of up to 32 VLAN items in this version and later.

Command changes

Modified command: vlan

Old syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

New syntax

vlan { *vlan-id-list*] | **all** }

undo vlan { *vlan-id-list* | **all** }

Views

System view

Change description

Before modification: The *vlan-id1* **to** *vlan-id2* option specifies a VLAN range. This option can be specified only once.

After modification: The *vlan-id-list* argument specifies a space-separated list of up to 32 VLAN items.

Modified feature: Displaying history about ports that are blocked by spanning tree protection features

Feature change description

You can use the **display stp abnormal-port** command to display history about ports that are blocked by spanning tree protection features.

Command changes

Modified command: display stp abnormal-port

Syntax

display stp abnormal-port

Views

Any view

Change description

Before modification:

```
<Sysname> display stp abnormal-port
 MST ID      Blocked Port                    Reason
 1           GigabitEthernet1/0/1            Root-Protected
 2           GigabitEthernet1/0/2            Loop-Protected
 12          GigabitEthernet1/0/3            Loopback-Protected
```

After modification:

```
<Sysname> display stp abnormal-port
---[GigabitEthernet1/0/1]---
```

```
    MST ID   BlockReason                    Time
    0        Loopback-Protected             07:56:44 05/01/2017
    0        Disputed                       07:56:37 05/01/2017
    0        Loop-Protected                 06:56:13 05/01/2017
---[GigabitEthernet1/0/2]---
    MST ID   BlockReason                    Time
    0        Loopback-Protected             07:55:51 05/01/2017
```

Modification:

- In an MSTI or VLAN, this command can display a maximum of three history records for a port that is blocked by spanning tree protection features.
- The following fields were added to the output from the **display stp abnormal-port** command:
  - **BlockReason**—Reason that the port was blocked.
  - **Time**—Protection feature trigger time.

Modified feature: Setting the LLDP frame transmission interval

Feature change description

The minimum LLDP frame transmission interval was changed from 5 seconds to 1 second.

Command changes

Modified command: lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

Views

System view

Change description

Before modification: The value range for the *interval* argument was 5 to 32768 seconds.

After modification: The value range for the *interval* argument is 1 to 32768 seconds.

Modified feature: Displaying ARP entries

Feature change description

The unit of the displayed aging time for ARP entries was changed from minute to second, and Rule ARP entries were added to the output.

Command changes

Modified command: display arp

Syntax

display arp [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

Views

Any view

Change description

Before modification:

Display brief information about all ARP entries.

```
<Sysname> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface              Aging Type
20.1.1.1         00e0-fc00-0001  N/A      N/A                    N/A   S
193.1.1.70       00e0-fe50-6503  100      GE1/0/1                N/A   IS
192.168.0.115    000d-88f7-9f7d  1        GE1/0/2                18    D
192.168.0.39     0012-a990-2241  1        GE1/0/3                20    D
22.1.1.1         010c-299d-c041  10       N/A                    N/A   M
```

Display detailed information about all ARP entries.

```
<Sysname> display arp all verbose
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface              Aging Type
Vpn Instance
20.1.1.1         00e0-fc00-0001  N/A      N/A                    N/A   S
[No Vrf]
193.1.1.70       00e0-fe50-6503  100      GE1/0/1                N/A   IS
[No Vrf]
192.168.0.115    000d-88f7-9f7d  1        GE1/0/2                18    D
[No Vrf]
192.168.0.39     0012-a990-2241  1        GE1/0/3                20    D
[No Vrf]
22.1.1.1         010c-299d-c041  10       N/A                    N/A   M
[No Vrf]
```

After modification:

Display brief information about all ARP entries.

```
<Sysname> display arp all
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address       MAC Address     VID      Interface/Link ID      Aging Type
1.1.1.1          02e0-f102-0023  1        GE1/0/1                N/A   S
1.1.1.2          00e0-fc00-0001  12       GE1/0/2                960   D
1.1.1.3          00e0-fe50-6503  12       Tunnel1                960   D
1.1.1.4          000d-88f7-9f7d  12       0x1                    960   D
```

Display detailed information about all ARP entries.

```
<Sysname> display arp all verbose
```

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP Address       : 1.1.1.1          VID : 1           Aging   : N/A
MAC Address      : 02e0-f102-0023   Type: S           Nickname: 0x0000
Interface/Link ID: GE1/0/1
VPN Instance     : [No Vrf]
VXLAN ID         : N/A
VSI Name         : N/A
VSI Interface    : N/A
IP Address       : 1.1.1.2          VID : 12          Aging   : 960 sec
MAC Address      : 0015-e944-adc5   Type: D           Nickname: 0x0000
Interface/Link ID: GE1/0/2
VPN Instance     : [No Vrf]
VXLAN ID         : N/A
VSI Name         : N/A
VSI Interface    : N/A
IP Address       : 1.1.1.3         VID : 12          Aging   : 960 sec
MAC Address      : 0013-1234-0001  Type: D           Nickname: 0x0000
Interface/Link ID: Tunnel1
VPN Instance     : [No Vrf]
VXLAN ID         : N/A
VSI Name         : N/A
VSI Interface    : N/A
IP Address       : 1.1.1.4         VID : 12          Aging   : 960 sec
MAC Address      : 0012-1234-0002  Type: D           Nickname: 0x0000
Interface/Link ID: 0x1
VPN Instance     : [No Vrf]
VXLAN ID         : N/A
VSI Name         : N/A
VSI Interface    : N/A
```

The following changes were added to the command output:

- The **R-Rule** field was added.
- The unit of the displayed aging time for ARP entries was changed from minute to second.

Modified feature: Displaying the aging time of dynamic ARP entries

Feature change description

The unit of the displayed aging time of dynamic ARP entries was changed from minute to second.

Command changes

Modified command: display arp timer aging

Syntax

display arp timer aging

Views

Any view

Change description

Before modification: The unit of the displayed aging time of dynamic ARP entries was minute.

Display the aging time of dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 20 minute(s)
```

After modification: The unit of the displayed aging time of dynamic ARP entries was changed from minute to second.

Display the aging time of dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 1200 seconds
```

Modified feature: Default source IP address in packets relayed to the DHCP server

Feature change description

For the default source IP address in packets that the DHCP relay agent forwards to the DHCP server, the following changes have been made:

- In software versions earlier than Release 3207, the default source IP address is the IP address of the interface through which the DHCP relay agent connects the DHCP client.
- In Release 3207 and later, the default source IP address is the IP address of the output interface through which the DHCP relay agent forwards the packets to the DHCP server. You can use the **dhcp relay source-address** command to modify the source IP address for these relayed packets.

Command changes

None.

Modified feature: Specifying gateways on the DHCP server for DHCP clients

Feature change description

The maximum number of gateways that can be specified on the DHCP server for DHCP clients was changed from 8 to 64.

Command changes

Modified command: gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

Views

DHCP address pool view

DHCP secondary subnet view

Change description

Before modification: A maximum of eight gateways can be specified on the DHCP server for DHCP clients.

After modification: A maximum of 64 gateways can be specified on the DHCP server for DHCP clients.

Modified feature: Displaying information for DHCP snooping trusted ports

Feature change description

From this version, you can display VLAN information for DHCP snooping trusted ports.

Command changes

Modified command: display dhcp snooping trust

Syntax

display dhcp snooping trust

Views

Any view

Change description

Before modification:

Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
 DHCP snooping is enabled.
 Interface                                Trusted
 ========================                 ============
 GigabitEthernet1/0/1                     Trusted
```

After modification:

Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
 DHCP snooping is enabled.
 Interface                                Trusted          VLAN
 ========================                 ============     =======
 GigabitEthernet1/0/1                     Trusted
 GigabitEthernet1/0/2                     -                100
 GigabitEthernet1/0/3                     -                100, 200
```

The following changes were added to the command output:

- **Trusted**—For a DHCP snooping trusted port configured in system view, this field displays **Trusted**. For a trusted port configured in VLAN view, this field displays a hyphen (**-**).
- **VLAN**—VLANs in which the port is configured as trusted. If a trusted port is configured after DHCP snooping is enabled globally, this field is empty.

Modified feature: Setting the MTU of IPv4 packets sent over an interface

Feature change description

The value range for the MTU of IPv4 packets sent over an interface was changed.

Command changes

Modified command: ip mtu

Syntax

ip mtu *mtu-size*

undo ip mtu

Views

Interface view

Change description

Before modification: The value range for the *mtu-size* argument is 128 to 2000 bytes.

After modification: The value range for the *mtu-size* argument is 128 to 1500 bytes.

Modified feature: Setting the TCP buffer size

Feature change description

The default size of the TCP receive/send buffer was changed from 64 KB to 63 KB.

Command changes

Modified command: tcp window

Syntax

tcp window *window-size*

undo tcp window

Views

System view

Change description

Before modification: The default size of the TCP receive/send buffer is 64 KB.

After modification: The default size of the TCP receive/send buffer is 63 KB.

Modified feature: Configuring prefix to be advertised in RA messages

Feature change description

The following changes were added to the **ipv6 nd ra prefix** command:

- The **no-advertise** keyword was added.
- The *valid-lifetime*, *preferred-lifetime*, and **no-advertise** parameters in this command were changed from required to optional.

Command changes

Modified command: ipv6 nd ra prefix

Old syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

New syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

Views

Interface view

Change description

Before modification:

- The device always advertises the prefix in RA messages.
- When configuring the **ipv6 nd ra prefix** command, you must specify the *valid-lifetime* and *preferred-lifetime* parameters.

After modification:

- The **no-advertise** keyword was added to disable the device from advertising the prefix specified in the **ipv6 nd ra prefix** command.
- The *valid-lifetime* and *preferred-lifetime* parameters become optional. If you do not configure optional parameters for this command, the prefix uses the default settings configured by the **ipv6 nd ra prefix default** command.

Modified feature: Setting the MTU of IPv6 packets sent over an interface

Feature change description

The value range for the MTU of IPv6 packets sent over an interface was changed.

Command changes

Syntax

ipv6 mtu *size*

undo ipv6 mtu

Views

Interface view

Change description

Before modification: The value range for the *size* argument is 1280 to 10240 bytes.

After modification: The value range for the *size* argument is 1280 to 1500 bytes.

Modified feature: Displaying PBR configuration

Feature change description

In this release, the **display ip policy-based-route setup** command can display the type of the policies.

Command changes

Modified command: display ip policy-based-route setup

Syntax

display ip policy-based-route setup

Views

Any view

Change description

Before modification: The command displays applied policies and interfaces to which the policies are applied.

```
<Sysname> display ip policy-based-route setup
Policy Name              Interface Name
pr01                     Vlan-interface 1
```

After modification: The command displays applied policies, interfaces to which the policies are applied, and type of the policies.

```
<Sysname> display ip policy-based-route setup
Policy name              Type     Interface
pr01                     Forward  Vlan-interface2
aaa                      Local    N/A
```

Table 12 Command output

Field	Description
Type	Type of the PBR: • **Forward**—Interface PBR. • **Local**—Local PBR.

Modified feature: Displaying IPv6 PBR configuration

Feature change description

In this release, the **display ipv6 policy-based-route setup** command can display the type of the policies.

Command changes

Modified command: display ipv6 policy-based-route setup

Syntax

display ipv6 policy-based-route setup

Views

Any view

Change description

Before modification: The command displays applied IPv6 policies and interfaces to which the IPv6 policies are applied.

```
<Sysname> display ipv6 policy-based-route setup
Policy Name              Interface Name
pr01                     Vlan-interface 1
```

After modification: The command displays applied IPv6 policies, interfaces to which the IPv6 policies are applied, and type of the IPv6 policies.

```
<Sysname> display ipv6 policy-based-route setup
Policy name              Type               Interface
pr01                     Forward            Vlan-interface 2
pr02                     Local              N/A
```

Table 13 Command output

Field	Description
Type	Type of the IPv6 PBR: • **Forward**—Interface IPv6 PBR. • **Local**—Local IPv6 PBR.

Modified feature: Creating an ACL

Feature change description

The syntax of the **acl** command was changed.

Command changes

Modified command: acl

Old syntax

acl [**ipv6**] **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

New syntax

acl [**ipv6**] { **advanced** | **basic** } { *acl*-**number** | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl [**ipv6**] **number** *acl-number* [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

undo acl [**ipv6**] **number** *acl-number*

Views

System view

Change description

After modification:

- You can use the **acl** [**ipv6**] **number** *acl-number* command to create an ACL or enter the view of an existing ACL.
- If an ACL is created by using the **name** *acl-name* option, you can use only the **acl** [**ipv6** | **mac**] **name** *acl-name* command to enter the ACL view.

Modified feature: Copying an ACL to create a new ACL

Feature change description

The syntax of the **acl copy** command was changed.

Command changes

Modified command: acl copy

Old syntax

acl [**ipv6**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

New syntax

acl [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Views

System view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Displaying ACL configuration and match statistics

Feature change description

The syntax of the **display acl** command was changed.

Command changes

Modified command: display acl

Old syntax

display acl [**ipv6**] { *acl-number* | **all** | **name** *acl-name* }

New syntax

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

Views

Any view

Change description

After modification:

- The **mac** keyword was required to specify a Layer 2 ACL.
- The start rule ID was added in the command output.

Modified feature: Displaying packet filtering statistics

Feature change description

The syntax of the **display packet-filter statistics** command was changed.

Command changes

Modified command: display packet-filter statistics

Old syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**brief**]

New syntax

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]

Views

Any view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Displaying accumulated packet filtering statistics for an ACL

Feature change description

The syntax of the **display packet-filter statistics sum** command was changed.

Command changes

Modified command: display packet-filter statistics sum

Old syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6**] { *acl-number* | **name** *acl-name* } [**brief**]

New syntax

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]

Views

Any view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Displaying ACL application details for packet filtering

Feature change description

The syntax of the **display packet-filter verbose** command was changed.

Command changes

Modified command: display packet-filter verbose

Old syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

New syntax

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

Views

Any view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Applying an ACL to an interface for packet filtering

Feature change description

The syntax of the **packet-filter** command was changed.

Command changes

Modified command: packet-filter

Old syntax

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

New syntax

packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

Views

Layer 2 Ethernet interface view

VLAN interface view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Specify the applicable scope of packet filtering on a VLAN interface

Feature change description

The syntax of the **packet-filter filter** command was changed.

Command changes

Modified command: packet-filter filter

Old syntax

packet-filter filter [**route** | **all**]

New syntax

packet-filter filter { **route** | **all** }

Views

VLAN interface view

Change description

After modification, you must specify the application scope for packet filtering on a VLAN interface.

Modified feature: Clearing statistics for ACLs

Feature change description

The syntax of the **reset acl counter** command was changed.

Command changes

Modified command: reset acl counter

Old syntax

reset acl [**ipv6**] **counter** { *acl-number* | **all** | **name** *acl-name* }

New syntax

reset acl [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

Views

User view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Clearing the packet filtering statistics and accumulated statistics for an ACL

Feature change description

The syntax of the **reset packet-filter statistics** command was changed.

Command changes

Modified command: reset packet-filter statistics

Old syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6**] { *acl-number* | **name** *acl-name* }]

New syntax

reset packet-filter statistics interface [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

Views

User view

Change description

After modification, the **mac** keyword was required to specify a Layer 2 ACL.

Modified feature: Specifying an ACL match criterion

Feature change description

The syntax for specifying an ACL match criterion was changed.

Command changes

Modified command: if-match acl

Old syntax

if-match acl [**ipv6**] { *acl-number* | **name** *acl-name* }

New syntax

if-match acl [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }

Views

Traffic class view

Change description

The **mac** keyword was added to the **if-match acl** command for specifying a Layer 2 ACL.

Modified feature: Displaying predefined control plane QoS policies of cards

Feature change description

The **display qos policy control-plane pre-defined** command output was changed.

Command changes

Modified command: display qos policy control-plane pre-defined

Syntax

display qos policy control-plane pre-defined [**slot** *slot-number*]

Views

Any view

Change description

Command output before modification:

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority   Bandwidth (kbps)   Group
  IS-IS             4          512                critical
  VRRP              5          768                important
  IGMP              3          256                important
  VRRPv6            3          768                important
  ARP               1          256                normal
  DHCP Snooping     3          256                redirect
  DHCP              3          256                normal
  802.1x            1          128                important
  STP               6          256                critical
  LACP              5          64                 critical
  MVRP              3          256                critical
  BGP               3          256                critical
  ICMP              1          640                monitor
  IPOPTION          2          64                 normal
  BGPv6             3          256                critical
  IPOPTIONv6        2          64                 normal
  LLDP              3          128                important
  DLDP              3          64                 critical
  TELNET            1          512                management
  SSH               1          512                management
  HTTP              1          64                 management
  HTTPS             1          64                 management
  ARP Snooping      1          256                redirect
  ICMPv6            1          512                monitor
  DHCPv6            3          256                normal
```

Command output after modification:

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority   Bandwidth          Group
  Default           N/A        0 (kbps)           N/A
  IS-IS             4          512 (kbps)         critical
  VRRP              35         768 (kbps)         important
  IGMP              3          256 (kbps)         important
  VRRPv6            35         768 (kbps)         important
```

```
ARP               1          128 (kbps)         normal
DHCP Snooping     3          256 (kbps)         redirect
DHCP              3          256 (kbps)         normal
802.1x            1          128 (kbps)         important
STP               6          256 (kbps)         critical
LACP              5          64 (kbps)          critical
MVRP              3          256 (kbps)         critical
BGP               3          256 (kbps)         critical
ICMP              1          640 (kbps)         monitor
IPOPTION          2          64 (kbps)          normal
BGPv6             3          256 (kbps)         critical
IPOPTIONv6        2          64 (kbps)          normal
LLDP              3          128 (kbps)         important
DLDP              3          64 (kbps)          critical
TELNET            1          512 (kbps)         management
SSH               1          512 (kbps)         management
TACACS            1          512 (kbps)         management
RADIUS            1          512 (kbps)         management
HTTP              1          64 (kbps)          management
HTTPS             1          64 (kbps)          management
ARP Snooping      1          256 (kbps)         redirect
ICMPv6            1          512 (kbps)         monitor
DHCPv6            3          256 (kbps)         normal
```

Modified feature: Length range for an ISP domain

Feature change description

The length range for an ISP domain name was changed.

Command changes

Modified commands: display domain, domain, domain default enable, domain if-unknown

Syntax

Any view:

display domain [*isp-name*]

System view:

domain *isp-name*

domain default enable *isp-name*

domain if-unknown *isp-name*

Views

Any view

System view

Change description

Before modification: The *isp-name* argument is a string of 1 to 24 characters.

After modification: The *isp-name* argument is a string of 1 to 255 characters.

Modified feature: Displaying local user configuration

Feature change description

Syntax was changed for the **display local-user** command to display local user configuration.

Command changes

Modified command: display local-user

Old syntax

display local-user [**class** { **manage** | **network** } | **service-type** { **ftp** | **http** | **https** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*]

New syntax

display local-user [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]

Views

Any view

Change description

Before modification:

- You cannot specify local users by the status of the idle cut feature.
- The **user-name** *user-name* option specifies all local users that have the specified username.

After modification:

- The **idle-cut** { **disable** | **enable** } option was added. This option specifies local users by the status of the idle cut feature.
- The **class** { **manage** | **network** } option was added before the **user-name** *user-name* option to specify device management users or network access users that have the specified username.

Modified feature: Displaying user group configuration

Feature change description

Syntax was changed for the **display user-group** command to display user group configuration.

Command changes

Modified command: display user-group

Old syntax

display user-group [*group-name*]

New syntax

display user-group { **all** | **name** *group-name* }

Views

Any view

Change description

Before modification: The *group-name* argument is optional. If you do not specify a user group, this command displays configuration for all user groups.

After modification:

- The **all** keyword was added. This keyword specifies all user groups.
- The **name** keyword was added before the *group-name* argument to specify a user group.
- You must specify either **all** or **name** *group-name*.

Modified feature: Enabling the RADIUS server load sharing feature

Feature change description

Syntax was changed for the command that enables the RADIUS server load sharing feature.

Command changes

Modified command: server-load-sharing enable

Old syntax

algorithm loading-share enable

undo algorithm loading-share enable

New syntax

server-load-sharing enable

undo server-load-sharing enable

Views

RADIUS scheme view

Change description

The syntax of this command was change from **algorithm loading-share enable** to **server-load-sharing enable**.

Modified feature: Setting the real-time accounting interval

Feature change description

Syntax was changed for the command that sets the real-time accounting interval, and the value range for the argument in this command was also changed.

Command changes

Modified command: timer realtime-accounting

Old syntax

timer realtime-accounting *minutes*

New syntax

timer realtime-accounting *interval* [**second**]

Views

RADIUS scheme view

Change description

Before modification:

- The value range for the *minutes* argument is 0 to 60.
- The real-time accounting interval is in minutes.

After modification:

- The value range for the *interval* argument is 0 to 71582.
- The **second** keyword was added. This keyword specifies the real-time accounting interval, in seconds. If you do not specify this keyword, the real-time accounting interval is in minutes.

Modified feature: Displaying 802.1X information

Feature change description

The **Max 802.1X users** field was removed from the output of the **display dot1x** command.

Command changes

Modified command: display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

Views

Any view

Change description

Before modification: The **Max 802.1X users** field in the command output indicates the maximum number of online 802.1X users each device supports.

After modification: The **Max 802.1X users** field is removed from the command output. The output does not include the information about the maximum number of online 802.1X users each device supports.

Modified feature: Port-specific mandatory 802.1X authentication domain

Feature change description

The length range was changed for the ISP domain name string when you specify a mandatory 802.1X authentication domain on a port.

Command changes

Modified command: dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the *domain-name* argument is 1 to 24 characters.

After modification: The value range for the *domain-name* argument is 1 to 255 characters.

Modified feature: Removing users from the MAC authentication critical VLAN on a port

Feature change description

The syntax was changed for the command that removes users from the MAC authentication critical VLAN on a port.

Command changes

Modified command: reset mac-authentication critical vlan

Old syntax

reset mac-authentication critical-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

New syntax

reset mac-authentication critical vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

Views

User view

Change description

The **critical-vlan** keyword was changed to **critical vlan**.

Modified feature: Port security's limit on the number of secure MAC addresses on a port

Feature change description

The value range was changed for setting the maximum number of secure MAC addresses that port security allows on a port.

Command changes

Modified command: port-security max-mac-count

Syntax

port-security max-mac-count *max-count*

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the *max-count* argument is 1 to 4294967295.

After modification: The value range for the *max-count* argument is 1 to 2147483647.

Modified feature: Enabling the SSH server to support SSH1 clients

Feature change description

From this release, the SSH server does not support SSH1 clients by default.

Command changes

Modified command: ssh server compatible-ssh1x

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

Views

System view

Change description

Before modification: The SSH server supports SSH1 clients by default.

After modification: The SSH server does not support SSH1 clients by default.

Modified feature: Creating an SSH user and specifying the service type and authentication method

Feature change description

Support for specifying multiple SSH client public keys was added for an SSH user.

Command changes

Modified command: ssh user

Old syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname* }] }

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey** [**assign** { **pki-domain** *domain-name* | **publickey** *keyname* }] }

New syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey** [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

Views

System view

Change description

After modification, you can specify multiple SSH client public keys for client verification.

Modified feature: Predefined user roles for SSH and FTP client commands

Feature change description

The predefined user roles for the following SSH and FTP client commands were changed:

- **bye**
- **exit**
- **help**
- **quit**

Command changes

Modified command: bye

Syntax

bye

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

Modified command: exit

Syntax

exit

Views

SFTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

Modified command: help

Syntax

help

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

Modified command: quit

Syntax

quit

Views

SFTP client view

FTP client view

Change description

Before modification, the predefined user role for this command is network-admin.

After modification, the predefined user roles for this command are network-admin and network-operator.

Modified feature: Setting the number of ARP blackhole route probes for each unresolved IP address

Feature change description

The default value of ARP blackhole route probes for each unresolved IP address was changed from one to three.

Command changes

Modified command: arp resolving-route probe-count

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

Views

System view

Change description

Before modification: The device performs one ARP blackhole route probe for each unresolved IP address by default.

After modification: The device performs three ARP blackhole route probes for each unresolved IP address by default.

Modified feature: Displaying information about SNMPv1 or SNMPv2c communities

Feature change description

The **ACL name** field was added to the output from the **display snmp-agent community** command.

Command changes

Modified command: display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

Views

Any view

Change description

Before modification:

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1
```

After modification:

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       ACL:2001
       Storage-type: nonVolatile
       Context name: con1

   Community name: cc
       Group name: cc
       ACL name: testacl
       Storage-type: nonVolatile
```

The **ACL name** field appears only when an ACL name is specified for the SNMPv1 or SNMPv2c community. It is exclusive with the **ACL** field.

Modified feature: Displaying information about SNMP groups

Feature change description

The **ACL name** field was added to the output from the **display snmp-agent group** command.

Command changes

Modified command: display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

Views

Any view

Change description

Before modification:

```
<Sysname> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile
```

After modification:

```
<Sysname> display snmp-agent group
   Group name: groupv3
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview: <no specified>
       Storage-type: nonVolatile
       ACL name: testacl
```

The **ACL name** field appears only when an ACL name is specified for the SNMP group. It is exclusive with the **ACL** field.

Modified feature: Displaying SNMPv3 user information

Feature change description

The **ACL name** field was added to the output from the **display snmp-agent usm-user** command.

Command changes

Modified command: display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Views

Any view

Change description

Before modification:

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
```

After modification:

```
<Sysname> display snmp-agent usm-user
   Username: userv3
   Group name: mygroupv3
       Engine ID: 800063A203000FE240A1A6
       Storage-type: nonVolatile
       UserStatus: active
       ACL: 2000
   Username: userv3
   Group name: mygroupv3
       Engine ID: 8000259503000BB3100A508
       Storage-type: nonVolatile
       UserStatus: active
       ACL name: testacl
```

The **ACL name** field appears only when an ACL name is specified for the SNMPv3 user. It is exclusive with the **ACL** field.

Modified feature: Configuring an SNMPv1 or SNMPv2c community

Feature change description

The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options and advanced ACLs were supported for configuring an SNMP community.

Command changes

Modified command: snmp-agent community

Old syntax

In VACM mode:

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

In RBAC mode:

snmp-agent community [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

New syntax

In VACM mode:

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

In RBAC mode:

snmp-agent community [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMP community.

After modification:

- You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMP community.
- You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMP community.

Modified feature: Creating an SNMP group

Feature change description

The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options and advanced ACLs were supported for creating an SNMP group.

Command changes

Modified command: snmp-agent group

Old syntax

SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

SNMPv3 (in non-FIPS mode):

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

SNMPv3 (in FIPS mode):

snmp-agent group v3 *group-name* { **authentication** | **privacy** } [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

New syntax

SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

SNMPv3 (in non-FIPS mode):

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

SNMPv3 (in FIPS mode):

snmp-agent group v3 *group-name* { **authentication** | **privacy** } [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMP group.

After modification:

- You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMP group.
- You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMP group.

Modified feature: Creating an SNMPv1 or SNMPv2c user

Feature change description

The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options and advanced ACLs were supported for creating an SNMPv1/SNMPv2c user.

Command changes

Modified command: snmp-agent usm-user { v1 | v2c }

Old syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

New syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMPv1/SNMPv2c user.

After modification:

- You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMPv1/SNMPv2c user.
- You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMPv1/SNMPv2c user.

Modified feature: Creating an SNMPv3 user

Feature change description

The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options and advanced ACLs were supported for creating an SNMPv3 user.

The following encryption algorithms were added for creating an SNMPv3 user:

- **In FIPS mode—aes192** and **aes256** encryption algorithms.
- **In non-FIPS mode—3des**, **aes192**, and **aes256** encryption algorithms in VACM mode and **aes192** and **aes256** encryption algorithms in RBAC mode.

Command changes

Modified command: snmp-agent usm-user v3

Old syntax

In non-FIPS mode (in VACM mode):

snmp-agent usm-user v3 *user-name group-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

In non-FIPS mode (in RBAC mode):

snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **3des** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

In FIPS mode (in VACM mode):

snmp-agent usm-user v3 *user-name group-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* }] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode aes128** *priv-password*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

In FIPS mode (in RBAC mode):

snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ip-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode aes128** *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *

New syntax

In non-FIPS mode (in VACM mode):

snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

In non-FIPS mode (in RBAC mode):

snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

In FIPS mode (in VACM mode):

snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

In FIPS mode (in RBAC mode):

snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* }] [{ **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

Views

System view

Change description

Before modification: You can specify a basic IPv4/IPv6 ACL by its number for an SNMPv3 user.

After modification:

- You can specify a basic or advanced IPv4/IPv6 ACL by its number for an SNMPv3 user user.
- You can specify a basic or advanced IPv4/IPv6 ACL by its name for an SNMPv3 user.

The following parameters were added to the command:

- **In FIPS mode**—The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options and the **aes192** and **aes256** keywords.
- **In non-FIPS mode**—The **name** *ipv4-acl-name* and **name** *ipv6-acl-name* options **and** the **3des, aes192**, and **aes256** keywords in VACM mode and **aes192** and **aes256** keywords in RBAC mode.

Modified feature: Configuration locking BY NETCONF

Feature change description

Before modification: After a user uses NETCONF to lock the configuration, other users cannot use NETCONF to configure the device but can use other configuration methods, such as CLI and SNMP.

After modification: After a user uses NETCONF to lock the configuration, other users cannot use NETCONF or any other methods to configure the device.

Command changes

None.

Modified feature: Value range for the interval for an OpenFlow instance to reconnect to a controller

Feature change description

The value range changed for the interval for an OpenFlow instance to reconnect to a controller.

Command changes

Modified command: controller connect interval

Syntax

controller connect interval *interval*

undo controller connect interval

Views

OpenFlow instance view

Change description

Before modification: The value range for the *interval* argument is 10 to 120 seconds.

After modification: The value range for the *interval* argument is 1 to 120 seconds.

Removed features

Table 14 Removed features in version R3207

Feature	Removed commands
IPv6 basics: Enabling a device to discard IPv6 packets that contain extension headers	The **ipv6 option drop enable** command was removed from system view.
QoS: Configuring traffic policing for all traffic on inbound interface by using the non-MQC approach	• The following commands were removed from Layer 2 Ethernet interface view: ◦ **qos car inbound any cir** *committed-information-rate* [**cbs**

Feature	Removed commands
	committed-burst-size [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] ○ **qos car inbound any cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] • The **display qos car interface** [*interface-type interface-number*] command was removed from any view.
QoS: Configuring the bandwidth guaranteeing group	• The **qos nni bandwidth** *bandwidth-value* command was removed from system view. • The **qos uni enable** command was removed from Layer 2 Ethernet interface view. • The following commands were removed from any view: ○ **display qos nni bandwidth** ○ **display qos uni interface** [*interface-type interface-number*]
AAA: Specifying a security policy server for a RADIUS scheme	The **security-policy-server** { *ipv4-address* | **ipv6** *ipv6-address* } command was removed from RADIUS scheme view.
IKE: Specifying a DH group for key negotiation in phase 1	In FIPS mode, the **group24** keyword was removed from the **dh** command in IKE proposal view.

Related documentation

This document introduces software feature changes between HPE 5130EI-CMW710-R3207 and later versions. For information about software feature changes between software versions earlier than HPE 5130EI-CMW710-R3207, see *HPE 5130EI-CMW710-R3115P08 Release Notes (Software Feature Changes)*.